LA PROPOSTA DI REGOLAMENTO SUGLI ORDINI DI PRODUZIONE E CONSERVAZIONE EUROPEI: COMMISSIONE, CONSIGLIO E PARLAMENTO A CONFRONTO

di Oscar Calavita
(Dottorando in Diritto processuale penale, Università di Torino)

1. Nel campo della cooperazione internazionale a livello unionale, l'ultimo ventennio, ha visto un sostanziale incremento della fiducia reciproca tra gli Stati membri e ha consentito di trasformare la veste della cooperazione giudiziaria da strumento di mutua assistenza a strumento di mutuo riconoscimento.

Inserendosi nel cammino già tracciato, la Commissione Europea ha depositato il 17 aprile 2018 la proposta COM(2018)225 di *regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* ("proposta della Commissione")[1].

La novità risiede innanzitutto nello strumento utilizzato: il regolamento, direttamente applicabile all'interno di ciascuno Stato membro senza l'intermediazione degli stessi. Per la prima volta, dunque, l'idea della Commissione è quella di garantire la totale fiducia e il completo mutuo riconoscimento delle decisioni giudiziarie.

In estrema sintesi, la proposta della Commissione prevede che l'autorità

[1] Proposta della Commissione europea di *regolamento del Parlamento Europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, del 17 aprile 2018, COM(2018)225.

giudiziaria inquirente ordini direttamente al prestatore di servizi del sistema informatico o telematico localizzato in un altro Stato la conservazione o la produzione degli *e-data* in proprio possesso, al fine di velocizzare l'acquisizione degli stessi nell'era digitale. L'autorità giudiziaria può emettere un ordine di conservazione europeo (OCE) e ingiungere a un prestatore di servizi di conservare prove elettroniche in vista di una successiva richiesta di produzione. Tale ultima richiesta si sostanzia in un ordine di produzione europeo (OPE), che consiste in una decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi di altro Stato membro di produrre prove elettroniche in suo possesso.

Gli ordini emessi sono, in seguito, trasmessi per mezzo dei relativi certificati (denominati rispettivamente, per OCE e OPE, EPOC-CR ed EPOC), il cui scopo è quello di «fornire tutte le informazioni necessarie al destinatario in un formato standardizzato, escludendo dati sensibili contenuti negli ordini di produzione e di conservazione come quelli relativi alla necessità o alla proporzionalità di tali provvedimenti investigativi, per evitare di compromettere la segretezza e il buon esito delle indagini»[2].

La proposta della Commissione è stata oggetto di ampie discussioni in seno al Consiglio dell'Unione Europea e al Parlamento, i quali hanno presentato talune proposte emendative del progetto iniziale che verranno analizzate nel presente contributo[3] e che nel prossimo futuro saranno discusse a un tavolo trilaterale avviato tra Commissione, Consiglio e Parlamento.

2. I recenti approdi europei e internazionali hanno sottolineato come la globalizzazione, il libero mercato, la libera circolazione delle persone all'interno dell'Unione Europea e gli strumenti tecnologici e informatici apportino innumerevoli benefici al benessere delle persone. Tuttavia, gli stessi sono veicolo di accrescimento della criminalità transnazionale che può porre in pericolo lo spazio di libertà, sicurezza e giustizia[4].

In particolare, la natura sempre più immateriale dei dati, spesso custoditi in sistemi privi di fisicità in server *cloud*, rischia di mettere in crisi il sistema tradizionale legato alla sovranità territoriale degli Stati membri nell'applicazione delle regole penali

[2] R. Pezzuto, *Accesso transazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione Europea al vaglio del Consiglio dell'Unione*, in *Dir. Pen. cont*, fasc. 2/2019, p. 80.

[3] Orientamento generale del Consiglio sulla proposta di *regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 6 e 7 dicembre 2018, 2018/0108(COD) e Progetto di Relazione Sippel sulla proposta di *regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 24 ottobre 2019, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD).

[4] V. Considerando da 1 a 7 Proposta della Commissione, cit.

e processuali penali. Si pensi, per fare un esempio, a una truffa online attuata mediante posta elettronica, il cui server si trova in uno Stato diverso da quello di residenza dell'autore del reato e della persona offesa. Se l'autore rimane ignoto, si potrebbe rendere necessario richiedere al *service provider* (SP), stabilito in uno Stato membro diverso da quello in cui si procede, i dati di *log* o delle operazioni effettuate, al fine di individuare il soggetto e incardinare un procedimento penale nei suoi confronti. Al fine di consentire questo atto investigativo in modo celere ed evitare le tempistiche dell'Ordine Europeo di Indagine (OEI)[5] – che possono essere eccessivamente lunghe[6] in relazione alla volatilità dei dati elettronici – la proposta della Commissione vuole fare in modo che l'autorità giudiziaria di uno Stato membro possa ingiungere a un *provider* stabilito in un differente Stato di conservare o produrre i dati, come se questo fosse stabilito nel Paese nel quale è incardinato il procedimento.

La Commissione, come detto, riprende alcuni recenti approdi europei e internazionali, i quali insistono sulla necessità di potenziare le tecniche di raccolta della prova elettronica a livello transnazionale[7].

In particolare, la settima adunanza plenaria dello *European Judicial Cybercrime Network* (EJCN) del 2019, con particolare riferimento al tema delle *e-evidence*, ha sottolineato come vi sia attualmente la prassi[8], prevista da alcuni Stati membri e da

[5] direttiva 2014/41/UE del Parlamento europeo e del Consiglio, *relativa all'ordine europeo di indagine penale*, del 03 aprile 2014, in GUUE L 130 del 01 maggio 2014, pp. 1-36.

[6] «Per ottenere prove elettroniche attraverso i canali della cooperazione giudiziaria occorre spesso molto tempo, più di quello per cui gli eventuali indizi rimangono a disposizione» (considerando 8 Proposta della Commissione, cit.).

[7] A tal riguardo si possono ricordare:

1) La conferenza di Amsterdam sulla giurisdizione nel cyberspazio *Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group* del 17 febbraio 2016, la quale ha concluso osservando come sia opportuno implementare la Convenzione di Budapest sul Cybercrime del 2001 con un nuovo protocollo, nel quale prevedere ordini di produzione internazionali e regimi semplificati di mutua assistenza, anche con richieste di conservazione indirizzate direttamente ai *provider*. In relazione alla proposta di nuovo protocollo v. *Cybercrime Convention Committee (T-CY). Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments* reperibile su https://www.coe.int/en/web/cybercrime/tcy;

2) *Council conclusions on improving criminal justice in cyberspace*, 09 giugno 2016, reperibile su https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf., che hanno evidenziato l'importanza delle prove elettroniche nei procedimenti penali per qualsiasi tipo di reato e la necessità di ottenerle in modo rapido ed effettivo, intensificando la cooperazione con i Paesi terzi e, soprattutto, in modo diretto con i *service provider*;

[8] Come evidenziato in dottrina «*while a raid on a company that refuses to produce requested documents would be a viable possibility, a raid on a data centre would not bring similar (if any) results, unless disproportionally significant forces are used to find the necessary data, potentially including heavy decrypting capacities, if that was possible at*» (S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order*, in *New Journal of European Criminal Law*, 2020, n. 11, p. 169).

Come riporta altra dottrina, una cooperazione diretta con i *service provider* è prevista come volontaria in Austria,

alcuni *provider*, di interloquire direttamente nel rapporto autorità giudiziaria-soggetto privato. Tuttavia, tale *modus operandi*, se da un lato può comportare vantaggi per gli inquirenti, dall'altro crea un enorme *vulnus* alle garanzie difensive di indagati e imputati, i quali rischiano di essere soggetti a trattamenti differenti sulla base di una (in)volontaria collaborazione del *service provider*. Pertanto, onde evitare discriminazioni, l'EJCN auspica standard minimi comuni nell'Unione Europea per la raccolta dei dati elettronici[9].

Sulla base di queste considerazioni, la proposta della Commissione «mira ad adattare i meccanismi di cooperazione all'era digitale, fornendo alle autorità giudiziarie e di contrasto gli strumenti per stare al passo con le attuali modalità di comunicazione dei criminali e combattere le forme moderne di criminalità»[10].

Devono innanzitutto evidenziarsi i vantaggi dell'utilizzo di un regolamento.

A tal proposito, la Commissione ha ritenuto di adottare lo strumento regolamentare proprio al fine di rafforzare il mutuo riconoscimento, in linea con quanto previsto dall'art. 82, paragrafo 1, TFUE, dal momento che lo stesso è direttamente applicabile e offre un maggior livello di chiarezza e armonicità del sistema: e ciò anche allo scopo di evitare interpretazioni divergenti degli Stati membri e scongiurare i «problemi di recepimento incontrati dalle decisioni quadro sul riconoscimento reciproco delle sentenze e delle decisioni giudiziarie» [11] – come successo in Italia ad esempio in tema di mandato di arresto europeo[12] – ponendosi così in convergenza con i principi di sussidiarietà e proporzionalità richiesti per l'emanazione di un regolamento europeo.

Lo strumento regolamentare, in altri termini, comporta numerosi benefici perché, in primo luogo, intercetta l'esigenza di rafforzare la fiducia reciproca tra gli

---

Bulgaria, Danimarca, Estonia, Finlandia, Grecia, Italia, Lussemburgo, Malta, Paesi Bassi, Repubblica Ceca, Romania, Slovenia, Svezia, Ungheria; mentre sarebbe obbligatoria in Belgio, Cipro, Francia, Lituania, Portogallo, Regno Unito e Spagna (B.J. Blažič-T. Klobučar, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communications Technology Law*, 2020, p. 73).

[9] *European Judicial Cybercrime Network - 7th Plenary Meeting- Eurojust, 14 – 15 November 2019*, reperibile su http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Documents/EJCN-plenary-outcome-2019-11_EN.pdf.

[10] Relazione alla Proposta della Commissione, cit., p. 2.

[11] Relazione alla Proposta della Commissione, cit., p. 6. La frammentarietà del quadro giuridico riverbera i propri effetti anche sui «prestatori di servizi che cercano di ottemperare alle richieste dei servizi di contrasto» (considerando 9 Proposta della Commissione, cit.).

[12] Emblematico sul punto il tema dei motivi di rifiuto alla consegna, previsti come obbligatori e facoltativi dalla decisione quadro 2002/584/GAI, mentre il testo originale dell'art. 18 l. 22 aprile 2005, n. 69, di recepimento della citata decisione quadro, aveva reso obbligatori tutti i motivi di rifiuto, anche quelli facoltativi. Il completo allineamento della normativa interna con quella sovrannazionale si è avuto solo recentemente ad opera del d.lgs. 2 febbraio 2021, n. 10, il quale ha sostanzialmente tradotto nella l. n. 69 del 2005 le previsioni della DQ 2002/584/GAI.

Stati avvertita in sede di cooperazione giudiziaria penale ormai da diversi anni. In secondo luogo, permette di eliminare quella frammentarietà del quadro giuridico attuale che «crea difficoltà per i prestatori di servizi che cercano di ottemperare alle richieste dei servizi di contrasto»[13] e che rischia di creare disuguaglianze a indagati e imputati. Inoltre, una normativa europea unica agevola la conclusione di accordi bilaterali o multilaterali tra UE e altri Stati: si pensi a un possibile accordo UE-USA circa l'acquisizione dei dati dai *provider* di Google e Facebook, anche alla luce del recente *Cloud Act* adottato negli Stati Uniti[14], che ha già condotto al *data-sharing agreement* USA-UK del 3 ottobre 2019[15].

Sotto altro aspetto, vi è tuttavia da domandarsi, così come evidenziato tanto dalla dottrina sovrannazionale[16] quanto da quella interna[17], se l'art. 82, paragrafo 1, consenta effettivamente una interlocuzione diretta pubblico-privato.

L'art. 82, paragrafo 1, TFUE stabilisce che «la cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie». Il riferimento alla «cooperazione giudiziaria» e al riconoscimento delle «sentenze e delle decisioni giudiziarie» sembrerebbe far riferimento esclusivamente a un riconoscimento in cui gli attori sono le competenti autorità giudiziarie, con la conseguenza che un rapporto pubblico-privato esulerebbe da tale ambito applicativo[18].

A detta lettura potrebbe affiancarsene un'altra, di segno opposto. Invero, si potrebbe argomentare che il reciproco riconoscimento non necessariamente debba implicare un formale passaggio ad opera di un'autorità giudiziaria (o equivalente), dal

---

[13] Considerando 9 Proposta della Commissione, cit.

[14] *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* del 23 marzo 2018, reperibile su https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

[15] *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* del 03 ottobre 2019, reperibile su https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

[16] G. Robinson, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review*, 2018, n. 3, p. 352.

[17] A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione Europea sugli ordini di produzione e conservazione di prove elettroniche* (e-evidence), in *Leg. Pen.*, 16 ottobre 2020, p. 13.

[18] G. Robinson, *The European Commission's e-Evidence Proposal*, op. cit., p. 352; A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria*, op. cit., p. 13; *European Data Protection Bord (EDPB)*, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), 26 settembre 2018, in *eevidence_opinion_final_en.pdf (europa.eu)*, p. 4; *LIBE Committee*, An assessment of the Commission's proposals on electronic evidence, in *An assessment of the Commission's proposals on electronic evidence (europa.eu)*, p. 30.

momento che sarebbe il regolamento – in un clima di fiducia reciproca e in un'ottica *ex ante* – a riconoscere a livello europeo un OPE o un OCE. In altre parole, il regolamento sarebbe esso stesso il fondamento del reciproco riconoscimento, a prescindere da una delibazione giudiziaria nello stato di esecuzione. E tale lettura potrebbe essere suffragata dallo stesso art. 82, paragrafo 1, TFUE, che nel suo proseguo prevede che il Parlamento e il Consiglio, adottando la procedura legislativa ordinaria, possano «definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria». Si potrebbe sostenere che, non essendovi il richiamo alla «cooperazione giudiziaria», il riconoscimento operi a prescindere da un'interlocuzione tra autorità e che, di conseguenza, si possa adottare la procedura legislativa ordinaria (nella specie, appunto, un regolamento) per imporre a un *service provider* di collaborare con un'autorità giudiziaria straniera.

Un ulteriore profilo potenzialmente problematico riguarda la tecnica normativa utilizzata nella redazione della proposta che, in alcuni punti, pare risentire di un approccio più vicino a una direttiva che a un regolamento. Se, da un lato, vi è un'omogeneizzazione dei requisiti per l'emissione e la trasmissione di un ordine, con regole valide su tutto il territorio europeo; dall'altro, vi sono aspetti importanti, quali le sanzioni e i rimedi, che sono rimessi alle legislazioni degli Stati membri[19]. Così ragionando, tuttavia, il regolamento si atteggia a direttiva e potrebbe creare non poche differenze tra i Paesi dell'Unione.

L'adozione di un regolamento nella cooperazione giudiziaria è una scelta coraggiosa, anche considerando le istanze sovraniste che stanno avanzando negli ultimi tempi: sarebbe forse più opportuno osare ancora di più e creare una disciplina europea unica che non demandi agli Stati membri un'integrazione nazionale, sebbene una tale impostazione potrebbe trovare lo scoglio (forse insuperabile) dell'art. 82, paragrafo 2, TFUE, il quale impone l'adozione di direttive (e non di regolamenti) al fine di armonizzare le discipline processuali nazionali.

3. La proposta della Commissione, definita in dottrina «per certi versi "minimalista" e per altri eccessivamente rigorosa»[20], si basa sull'inedito rapporto diretto tra l'autorità giudiziaria di uno Stato membro con il *service provider* di un altro Stato membro, in assenza di un controllo preventivo da parte dell'autorità dello Stato di esecuzione, che può essere chiamata in causa dallo stesso *provider* solo *ex post* e in determinati casi in cui pare esservi una palese violazione dei diritti fondamentali[21].

[19] S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., pp. 178 s.

[20] R.M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento* e-evidence, in *Cass. Pen.*, 2019, n. 3, p. 1359.

[21] Per un primo commento alla proposta della Commissione v. L. Buono, *The Genesis of the European Union's New Proposed Legal Insturment(s) on e-Evidence*, in *ERA Forum*, 2019, n. 19, pp. 307–312; E. Colombo, *Ordini*

3.1. Il dato informatico è per sua natura volatile, instabile e immateriale, riveste una dimensione transnazionale, può essere modificato, cancellato, trasferito o alterato rapidamente e richiede strumenti investigativi che consentano un intervento pressoché immediato per la loro acquisizione[22]. È sempre più frequente, inoltre, che non vi sia alcun collegamento territoriale tra il prestatore di servizi e l'utente, i quali, nella maggior parte dei casi, risiedono in Stati membri differenti.

L'OCE è disegnato con una veste fisiologicamente prodromica rispetto all'OPE, dal momento che interviene in una fase precedente e legata a doppio filo con l'ordine di produzione. Invero, la struttura più snella dell'OCE, che può non richiedere alcun intervento giurisdizionale[23], permette di congelare – per un massimo di sessanta giorni – i dati che possono venire richiesti per mezzo di un OPE, in attesa che quest'ultimo venga emesso da un'autorità giudiziale.

Si può notare, dunque, come la Commissione abbia voluto farsi carico del delicato problema dell'acquisizione delle *e-evidence* nel contesto infra-europeo, concedendo agli Stati membri uno strumento rapido volto ad acquisire, e ancora prima

---

europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento, in *Cass. Pen.*, 2019, n. 7, pp. 2722-2729; V. Frassen, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, in *www.europeanlawblog.eu*, 12 ottobre 2018; R.M. Geraci, *La circolazione transfrontaliera*, cit., pp. 1340-1362; M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio*: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. Pen. Cont.*, 2018, n. 5, pp. 277-294; L. Gómez Amigo, *Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima*, in *Revista Española de Derecho Europeo*, 2019, n. 71, pp. 1-31; J.H. Jeppesen-G. Nojeim, *Initial Observations on the European Commission's e-Evidence Proposals*, in *www.cdt.org*, 18 aprile 2018; J.H. Jeppesen-G. Nojeim, *Assessing the European Commission's E-Evidence Proposals on Ten Human Rights Criteria*, in *www.cdt.org*, 18 aprile 2018; F. La Chioma, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, in *www.magistratutraindipendente.it*, 6 giugno 2019; V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Criminal Law*, 2018, 25, pp. 263-265; L. Moxley, *EU Releasaes e-Evidence Proposal for Cross-Border Data Access*, in *www.insideprivacy.com*; O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence*: osservazioni a caldo e possibili sviluppi*, in *www.medialaws.eu*, 26 ottobre 2018, pp. 1-8; G. Robinson, *The European Commission's e-Evidence Proposal*, op. cit.; F. Ruggeri, *Novità. Il protocollo 16 alla Cedu in vigore dal 1° agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in *Cass. Pen.*, 2018, n. 7-8, pp. 2660-2663; S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., pp. 161-183.

[22] V. il considerando 7 Proposta della Commissione, cit.: «i servizi su rete possono essere forniti da qualsiasi luogo e non necessitano di un'infrastruttura fisica, di locali o personale nel paese di destinazione. Di conseguenza, le prove pertinenti sono spesso conservate al di fuori dello Stato che effettua le indagini o da un prestatore di servizi stabilito al di fuori di tale Stato. Sovente non esiste alcun altro collegamento tra il caso oggetto di indagine nello Stato interessato e lo Stato in cui si trova il luogo di conservazione o lo stabilimento principale del prestatore di servizi». Il considerando 8 Proposta della Commissione, cit. precisa che «per ottenere prove elettroniche attraverso i canali della cooperazione giudiziaria occorre spesso molto tempo, più di quello per cui gli eventuali indizi rimangono a disposizione».

[23] L'OCE può infatti essere emesso da un pubblico ministero senza la necessaria convalida postuma da parte di un giudice.

a conservare in attesta della produzione, i dati elettronici detenuti da un *service provider* stabilito in un Paese differente da quello nel quale si stanno svolgendo le indagini.

3.2. Generalmente i prestatori di servizi di una infrastruttura internet possono essere in possesso di una serie di dati che possono essere fondamentali nell'ambito di un procedimento penale, dal momento che permettono di identificare tanto gli autori quanto le vittime dei reati per i quali si procede, oltre a consentire la verifica delle operazioni che sono state effettuate per mezzo dei servizi offerti dal *provider* e i contenuti delle stesse.

La proposta della Commissione prevede, all'art. 2, una quadripartizione[24] della tipologia di dati richiedibili dall'autorità giudiziaria direttamente al *service provider* che si assesta su due livelli di intrusività nei diritti fondamentali: un primo livello è costituito dai dati relativi agli abbonati[25] e agli accessi[26], ritenuti dalla proposta di regolamento meno invasivi della sfera del singolo; il secondo livello, che incide maggiormente sulla tutela del dati personali, comprende i dati relativi alle operazioni[27] e ai contenuti[28-29].

In sostanza, quindi, le quattro categorie citate sembrano abbracciare ad ampio

[24] La quadripartizione è inusuale e tipica al tempo stesso. Il considerando 20 Proposta della Commissione, cit., infatti, sottolinea come i dati relativi agli abbonati, ai contenuti e alle operazioni siano usuali nella maggior parte degli Stati membri e negli USA, mentre la categoria riguardante i dati relativi agli accessi è del tutto inedita nel panorama internazionale.

[25] Ai sensi dell'art. 2, paragrafo 7, della proposta i dati relativi agli abbonati sono quelli che riguardano l'identità di un abbonato, nonché il tipo di servizio e la sua durata, compresi i dati tecnici ma ad eccezione delle password

[26] Tali dati hanno lo scopo di identificare un soggetto mediante il ricorso a *file* di *log-in* (connessione) e di *log-off* (disconnessione). Secondo il considerando 21 Proposta della Commissione, cit. «i dati relativi agli accessi tipicamente sono registrati nell'ambito di una registrazione di eventi (in altre parole un log server) per indicare l'inizio e la fine di una sessione di accesso utente a un servizio. Il più delle volte si tratta di un indirizzo IP (statico o dinamico) o altro identificatore che individua l'interfaccia di rete usata durante la sessione di accesso. Se l'utente è ignoto, spesso occorre ottenere tali dati prima di poter richiedere al prestatore di servizi i dati relativi agli abbonati correlati a quell'identificatore».

[27] Ai sensi dell'art. 2, paragrafo 9, Proposta della Commissione, cit. i dati relativi alle operazioni sono «i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi che servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituiscano dati relativi agli accessi».

[28] I dati relativi al contenuto comprendono una gamma residuale di informazioni, atteso che vengono definiti come «qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono» (art. 2, paragrafo 10).

[29] V. Considerando 23 Proposta della Commissione, cit., secondo cui «l'intensità dell'impatto sui diritti fondamentali varia, in particolare tra i dati relativi agli abbonati e i dati relativi agli accessi, da un lato, e i dati relativi alle operazioni e i dati relativi al contenuto, dall'altro».

raggio almeno la maggior parte dei dati posseduti da un prestatore di servizi, ad eccezione – pare – dei dati riferibili alla cronologia e alle ricerche effettuate[30], ma ricomprendendo i dati criptati, qualora il gestore in concreto abbia la chiave di decodificazione[31].

È però opportuno segnalare che i dati citati devono essere già detenuti dal *service provider* ai sensi della normativa applicabile[32]. All'autorità giudiziaria non è, infatti, consentito di imporre al prestatore di servizi di conservare dati in relazione ai quali non detiene alcun obbligo o richiedere la conservazione di dati che verranno registrati in un tempo futuro, così come non sono contemplate le intercettazioni in tempo reale dei flussi informatici o telematici.

Le citate limitazioni paiono garantire la proporzionalità dello strumento e ben contemperare il bilanciamento dei diritti che vengono in gioco. La conservazione di un dato ancora inesistente o lo svolgimento di intercettazioni di flussi telematici o informatici si ingeriscono nella sfera del singolo con un grado di intrusività (lesivo di vari diritti, tra cui quelli al domicilio digitale e alla riservatezza) ben più elevato rispetto alla conservazione di un dato già detenuto nei sistemi di un *service provider*. Pertanto, la limitazione ai soli dati già acquisiti è in linea con la *ratio* della proposta di regolamento ed evita di snaturarlo e renderlo uno strumento "orwelliano" privo di una doppia garanzia giurisdizionale nello Stato di emissione e in quello di esecuzione.

In ogni caso, l'obbligo di conservazione dei dati e le intercettazioni in tempo reale del traffico informatico o telematico potrebbero essere richiesti per mezzo di un OEI, che è uno strumento con un funzionamento diverso rispetto a un OPE o un OCE e che garantisce il citato doppio vaglio giurisdizionale.

Vi è da segnalare, tuttavia, che la definizione della tipologia di dati richiedibili è

[30] R.M. Geraci, *La circolazione transfrontaliera*, cit., p. 1361.

[31] In termini v. considerando 19 Proposta della Commissione. Sul punto è stato evidenziato che «evidente è la rilevanza di tali previsioni quando vengano in considerazione applicazioni, quali *Whatsapp* o *Skype*, che utilizzino tecniche di questo genere al fine di ostacolare l'accesso ai dati» (V. Dova, *L'accesso transfrontaliero all'*electronic evidence*, tra esigenze di effettività e tutela dei diritti*, in *Dir. Pen. cont. Riv. Trim.,* n. 2/2019, p. 449). Vi è, tuttavia, da precisare che taluni servizi criptati non possono essere decodificati dal gestore, bensì esclusivamente dagli utenti per mezzo di un codice univoco (si pensi alla crittografia end-to-end di Whatsapp). In simili situazioni, verosimilmente, non sarà possibile ottenere informazioni sul contenuto, ma solo la prova dell'esistenza che una determinata comunicazione è avvenuta.

[32] «Il presente regolamento disciplina l'acquisizione solo dei dati conservati, ossia dei dati detenuti dal prestatore di servizi al momento della ricezione di un certificato di ordine europeo di produzione o di conservazione. Non impone un obbligo generale di conservare i dati né autorizza l'intercettazione di dati o l'ottenimento di dati che saranno conservati dopo la ricezione del certificato di ordine di produzione o di conservazione. I dati devono essere forniti a prescindere dal fatto che siano criptati o meno» (considerando 19 Proposta della Commissione, cit.). In dottrina si è però evidenziato che «*one might wonder whether the traditional distinction between real-time collection of data and the gathering of stored data is still that relevant in a digital age. For certain types of data (e.g. emails and chat messages), it is not always clear whether they are 'in transmission' or already 'stored'*» (V. Frassen, *The European Commission's e-Evidence Proposal*, cit.).

stata oggetto di critiche tanto dallo *European Data Protection Supervisor* (EDPS)[33] quanto dalla dottrina, i quali hanno evidenziato come il regolamento dovrebbe definire più precisamente i contorni delle stesse, onde evitare di «porre sulle spalle del prestatore di servizi il compito di stabilire se i dati richiesti rientrino effettivamente nelle categorie contemplate dalla disciplina comunitaria oppure no»[34].

3.3. La proposta di regolamento ha efficacia nei confronti di alcune categorie di prestatori di servizi che operano sul territorio dell'Unione Europea (ad eccezione della Danimarca) o che hanno un "collegamento sostanziale" con la stessa, anche se stabiliti fisicamente in uno stato extra-UE: infatti, è opportuno precisare che il regolamento non si applica esclusivamente ai *service provider* stabiliti nell'Unione, ma è sufficiente che offrano servizi all'interno di essa, a prescindere dalla presenza di una struttura fisica nel vecchio continente[35].

È opportuno specificare che la proposta di regolamento della Commissione non consente alle autorità giudiziarie di emettere ordini nei confronti di tutti i prestatori di servizi indiscriminatamente, ma limita tale potere ad alcune categorie. A tal riguardo dispone l'art. 2, paragrafo 3, della proposta che definisce il prestatore di servizi come la persona fisica o giuridica che fornisce una serie determinata di servizi. Tra questi vanno annoverati: 1) i servizi di comunicazione elettronica come definiti dalla direttiva che istituisce il codice delle comunicazioni europeo, nei quali vanno annoverate le comunicazioni Voice over IP (VoIP), la messaggistica istantanea e i servizi di posta elettronica[36]; 2) i servizi della società dell'informazione per i quali la conservazione dei dati è una componente propria del servizio fornito dall'utente, tra cui i *social network*, i mercati online che agevolano le operazione tra utenti e altri prestatori di servizi di *hosting*; 3) i servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i *registrar* di nomi di dominio e i connessi servizi per la *privacy* o *proxy*. Esulano, invece, dall'applicazione del regolamento i servizi della società dell'informazione per i quali «la conservazione dei dati non è una componente propria del servizio fornito all'utente

[33] *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, n. 7/2019, Bruxelles, 06 novembre 2019, consultabile sul sito https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

[34] A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea*, op. cit., p. 16.

[35] S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., p. 172. Sul punto è opportune specificare che la Proposta della Commissione europea di *direttiva del Parlamento Europeo d del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, del 17 aprile 2018, COM(2018)226 impone ai provider che esercitano sul territorio unionale di nominare un legale rappresentante per ricevere gli ordini.

[36] Direttiva 2018/1972/UE del Parlamento europeo e del Consiglio, *che istituisce il codice europeo delle comunicazioni elettroniche*, del 11 dicembre 2018, in GUUE L 321 del 17 dicembre 2018, pp. 36-214.

bensì un elemento puramente accessorio, quali i servizi giuridici, architettonici, ingegneristici e contabili forniti online o a distanza»[37].

Quest'ultima eccezione pare fare adeguata applicazione del principio di proporzionalità, stante, da un lato, la delicatezza di alcuni temi e dati trattati nel corso di talune attività professionali (si pensi all'attività forense), e, dall'altro, l'onere eccessivo che graverebbe su soggetti per i quali la conservazione dei dati non rientra nel *core business*.

Inoltre, la richiesta di dati a determinate categorie di prestatori di servizi professionali tenuti al segreto professionale (avvocati, medici ecc..) rischierebbe di frustare completamente i diritti fondamentali del singolo e la finalità del segreto stesso. Sarebbe infatti inutile garantire *ex ante* e in costanza di mandato la segretezza di certi rapporti se in seguito il professionista è tenuto a fornire i dati relativi al contenuto di quanto in proprio possesso, anche in considerazione del fatto che i servizi professionali stanno assumendo un grado di informatizzazione sempre maggiore.

L'art. 2, paragrafo 4, della proposta, per stabilire l'ambito di applicazione del regolamento, prevede che il prestatore di servizi consenta alle persone fisiche o giuridiche residenti o stabilite in uno o più Stati membri di usufruire dei servizi sopracitati e abbia un collegamento sostanziale con questi ultimi.

Il collegamento sostanziale, se da un lato non pare porre problemi qualora un *provider* abbia un'infrastruttura stabile all'interno dell'Unione, dall'altro suscita questioni interpretativa in mancanza di quest'ultima.

Sul punto, infatti, il considerando 28 afferma che «il collegamento sostanziale dovrebbe essere valutato sulla base dell'esistenza di un numero significativo di utenti in uno o più Stati membri, o dell'orientamento delle attività verso uno o più Stati membri». Quest'ultimo può poi essere desunto dall'uso di una lingua o di una moneta presente dell'Unione, dalla possibilità di ordinare prodotti o servizi, dalla presenza di un'app nell'*app store*, dalla pubblicizzazione dei servizi a livello locale ovvero ancora dalla gestione della clientela nella lingua utilizzata in uno Stato membro. Tale collegamento immateriale dovrà essere riempito di contenuto da parte delle prime applicazioni concrete, in quanto l'elencazione dei criteri dai quali desumere il citato collegamento deve certamente ritenersi non esaustiva e, probabilmente, sarà terreno fertile per situazioni che, almeno in linea teorica, paiono difficilmente immaginabili.

3.4. Prima di passare ad analizzare nel dettaglio le procedure applicative dei due ordini è opportuno segnalare i requisiti minimi che sono comuni ad entrambi i nuovi strumenti.

Da un lato, l'OCE e l'OPE possono essere emessi solo nell'ambito di specifici

[37] Considerando 16 Proposta della Commissione, cit.

procedimenti penali in relazione a un reato che è già stato commesso[38], ai fini dell'acquisizione di mezzi istruttori detenuti all'estero. Dall'altro, il mezzo investigativo deve essere necessario e proporzionato (artt. 5, paragrafo 2, e 6, paragrafo 2, della proposta)[39].

Il requisito del procedimento penale, da intendersi in tutto il suo arco dalla fase preprocessuale (intesa, in Italia, come fase delle indagini preliminari) alla fase processuale – ad eccezione (pare) della fase esecutiva che solitamente non è ricompresa nella fase processuale *stricto sensu* intesa – (art. 3, paragrafo 2 della proposta), non permette di adottare gli ordini né in procedimenti riguardanti misure di prevenzione, né ai fini della ricerca del condannato, dell'internato, dell'imputato sottoposto a misura cautelare custodiale o del latitante[40].

Il riferimento a un reato già commesso e al procedimento penale, inoltre, vieta di utilizzare il nuovo strumento quale veicolo per indagini meramente esplorative volte alla ricerca di un fatto di reato o di utilizzarlo nell'ambito di un procedimento amministrativo o, comunque, differente da quello penale. Sul punto vi è dunque una netta inversione di tendenza rispetto a quanto previsto dalla direttiva 2014/41/UE, in relazione alla quale è prevista la possibilità che un OEI possa essere emesso anche in procedimenti avviati dalle autorità amministrative o da autorità giudiziarie diverse da quella penale.

La soluzione restrittiva formulata nella proposta della Commissione si apprezza perché evita che la compressione dei diritti fondamentali avvenga senza la presenza di esigenze che possano giustificarne il sacrificio e, al contempo, non impedisce che autorità amministrative o civili possano richiedere i dati detenuti dai *service provider* per mezzo di uno strumento che prevede un doppio vaglio di giurisdizionalità quale è l'OEI. Così operando, in altri termini, pare che venga garantito il principio di proporzionalità.

In ordine a quest'ultimo principio e a quello di necessità, il considerando 29 stabilisce che «la valutazione dovrebbe considerare se l'ordine è limitato a quanto necessario per raggiungere il legittimo obiettivo di ottenere i dati pertinenti e necessari che dovranno servire da prova solo nella singola fattispecie».

Per fornirne una definizione più accurata è tuttavia necessario richiamare gli approdi della giurisprudenza della Corte Europea dei Diritti dell'Uomo (Corte EDU)

[38] Considerando 24 Proposta della Commissione, cit.

[39] Considerando 24 e 29 Proposta della Commissione, cit.

[40] Evidenza F. La Chioma, *L'ordine di produzione e di conservazione*, op. cit., che il riferimento a un procedimento penale implica che non vi è la possibilità di utilizzare gli ordini «per fondare una legittimazione statuale ad esigere forme di collaborazione da privati volte alla fornitura di evidenze in relazione ad un'attività di monitoraggio preventivo di eventuali attività illecite che non hanno trovato preliminare consacrazione in un provvedimento di scrizione nel registro» degli indagati (il c.d. 335 c.p.p.).

che ha tratteggiato i requisiti minimi di legalità per la limitazione del diritto alla riservatezza e al rispetto della vita privata e familiare.

La necessità delle misure deve essere valutata alla luce degli obiettivi da perseguire in una società democratica, quali la pubblica sicurezza, il benessere economico del Paese, la difesa dell'ordine pubblico, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui (art. 8, paragrafo 2, CEDU). Più precisamente, la necessità in una società democratica implica un «bisogno sociale imperioso» che deve tenere conto del fatto che «un margine di apprezzamento viene lasciato alle autorità nazionali, la cui decisione rimane soggetta al controllo della Corte, competente per verificarne la conformità alle esigenze della Convenzione»[41]. Un margine di apprezzamento che è tanto più ristretto quanto più il diritto fondamentale che viene in gioco è sedimentato tra gli Stati del Consiglio d'Europa, come il diritto alla vita e all'identità dell'individuo, mentre è più ampio per taluni diritti, come quello alla libertà religiosa, che prevedono necessariamente una valutazione di ordine etico o morale.

La proporzionalità, invece, deve leggersi con riferimento allo scopo legittimo perseguito e richiede all'autorità giudiziaria competente di assicurare un giusto equilibrio tra gli interessi privati e quelli pubblici. In particolare, il vaglio di proporzionalità dovrebbe seguire lo schema tripartito ormai consolidato che prevede: 1) un controllo di idoneità dello strumento rispetto al fine perseguito; 2) una valutazione di stretta necessità, che prevede che se vi sono misure ugualmente idonee al raggiungimento dello scopo è necessario adottare quelle che comportano una lesione meno grave dei diritti fondamentali coinvolti; 3) un controllo di proporzionalità in senso stretto e che si sostanzia in una valutazione che risponde a un bilanciamento tra vantaggi ottenibili con lo strumento e svantaggi che incidono sui diritti fondamentali. Nel caso in cui i vantaggi siano maggiori degli svantaggi, allora la misura può considerarsi proporzionata[42].

È ancora opportuno precisare che gli OPE potranno essere emessi solo se la normativa interna preveda una misura dello stesso tipo in un caso interno analogo (art. 5, paragrafo 2, della proposta)[43], mentre gli OCE potranno essere adottati in relazione a qualsiasi reato (art. 6, paragrafo 2, della proposta)[44]. Una tale diversificazione di

[41] Corte europea dei diritti dell'uomo, Granze Camera, sentenza del 24 gennaio 2017, ricorso n. 25358/12, *Paradiso e Campanelli c. Italia*, par. 181.

[42] V., fra i molti, M. Daniele, *I chiaroscuri dell'OEI e la bussola della proporzionalità*, in M. Daniele-R.E. Kostoris (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transazionale delle prove nel d.lgs. n. 108 del 2017*, Torino, 2018, pp. 58-59; H.B. Havila, *Teoria dei principi*, trad. it., Torino, 2014, pp. 160-164.

[43] Il considerando 33 Proposta della Commissione, cit. stabilisce che «È inoltre necessario prevedere che l'ordine europeo di produzione possa essere emesso solo se un ordine dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione».

[44] «L'ordine europeo di conservazione può essere emesso per qualsiasi reato. Il suo scopo è impedire la

presupposti non pare convincere del tutto. Gli OCE, come visto, hanno una veste tendenzialmente prodromica rispetto a un successivo OPE e, dunque, vi è il rischio che un OCE possa essere richiesto in una situazione in cui un OPE (ovvero un OEI o una richiesta di assistenza giudiziaria tradizionale) non siano adottabili. Sarebbe perciò preferibile prevedere un "livellamento verso l'alto" delle condizioni per l'emissione di un OCE, parificando queste ultime a quelle previste per gli OPE. In tal modo, si garantirebbero maggiormente i diritti dei cittadini, in quanto si eviterebbero situazioni in cui i dati vengono conservati dai SP – su richiesta delle autorità giudiziarie – senza una successiva effettiva apprensione degli stessi a fini investigativi.

Tra i requisiti comuni alle due tipologie di ordini, come evidenziato in dottrina[45], manca un quadro indiziario minimo alla presenza del quale poter emettere un OCE o un OPE, similmente a quanto previsto dal codice di procedura penale italiano per le misure cautelari (gravi indizi di colpevolezza, art. 273 Cpp) e per le intercettazioni (gravi indizi di reato, art. 266 Cpp). Questa omissione è oggetto di proposta emendativa da parte del Parlamento, di cui si dirà in appresso.

Vi è, infine, da considerare che i destinatari degli ordini devono garantire la riservatezza dei dati prodotti o conservati e, su richiesta espressa dell'autorità emittente, al fine di non ostacolare il corretto corso procedimento penale, astenersi dal comunicare al soggetto interessato la trasmissione o la conservazione dei dati prodotti.

La previsione si pone in linea con quanto già previsto dall'art. 19 della direttiva OEI dedicato al tema della riservatezza delle indagini. Anche in tale contesto si focalizza l'attenzione sulla tematica specifica della segretezza delle indagini, che deve essere tenuta in debita considerazione al fine di assicurare il corretto esito dell'OEI, e si prevede altresì che «l'autorità di esecuzione garantisce, conformemente al proprio diritto nazionale, la riservatezza dei fatti e del contenuto dell'OEI, salvo nella misura necessaria all'esecuzione dell'atto di indagine» (art. 19, paragrafo 2, direttiva OEI). L'art. 11 della proposta, di conseguenza, pare effettuare un corretto bilanciamento tra diritti individuali e tutela del segreto istruttorio, in quanto si potrà derogare ai primi – e così posticipare l'attivazione dei rimedi nello Stato di emissione – solo nel momento

rimozione, la cancellazione o la modifica di dati pertinenti in situazioni in cui potrebbe occorrere più tempo per ottenere la loro produzione, ad esempio quando sono usati i canali della cooperazione giudiziaria» (considerando 36 Proposta della Commissione, cit.).

[45] «Sorprende come per l'adozione di entrambe le misure in discorso, al di là dei meri requisiti della necessità e proporzionalità delle stesse, non sia stato previsto uno standard probatorio minimo, richiedendosi ad esempio la sussistenza di un compendio indiziario in ordine al fatto per cui si procede a carico del titolare dei dati richiesti» (R.M. Geraci, *La circolazione transfrontaliera*, cit., p. 1360). Anche M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio, cit., p. 293 critica la mancata previsione di uno standard probatorio minimo, dal momento che «i soli parametri della "necessarietà e proporzionalità" rischiano, insomma, di essere troppo vaghi per riuscire a costituire un argine sufficiente per proteggere i diritti fondamentali degli accusati».

in cui ciò sia necessario al fine di non ostacolare il regolare esito del procedimento penale.

3.5. La procedura di emissione dell'ordine di conservazione europeo è descritta all'art. 6 e, per quanto riguarda l'autorità di emissione, all'art. 4 della proposta della Commissione.

In via preliminare, è fondamentale ribadire che la proposta presuppone che l'OCE abbia un'incidenza sui diritti fondamentali inferiore rispetto a quella dell'OPE e, per tale ragione, prevede condizioni per l'adozione meno stringenti rispetto a quest'ultimo strumento[46].

L'ordine di conservazione può essere adottato tanto da un organo giurisdizionale, da un magistrato inquirente o da un pubblico ministero quanto da un'altra autorità inquirente competente nello Stato di emissione. In quest'ultimo caso, tuttavia, l'OCE deve necessariamente essere convalidato *ex post* – ma prima della trasmissione del relativo certificato – da un giudice, da un organo giurisdizionale, da un magistrato inquirente o da un pubblico ministero (art. 4, paragrafo 3, della proposta), i quali devono essere considerati come autorità di emissione ai fini della trasmissione del certificato (art. 4, paragrafo 4, della proposta).

Come anticipato, pur suscitando alcune riserve, l'OCE può essere emesso in relazione a qualsiasi reato (art. 6, paragrafo 2, della proposta), quindi – deve ritenersi – anche per quelli di natura bagatellare[47], e deve essere necessario e proporzionato in relazione a uno specifico fine richiamato dall'art. 6, paragrafo 2, della proposta: «impedire la rimozione, la cancellazione o la modifica di dati» con l'obiettivo di richiederne l'acquisizione successivamente attraverso strumenti di assistenza giudiziaria tradizionali, un OEI o un OPE. La previsione dell'art. 6, paragrafo 2, della proposta della Commissione conferma, dunque, il carattere strumentale dell'OCE quale mezzo provvisorio, che congela il dato e lo rende immodificabile, in vista di una

[46] Sul punto v. i considerando 30 e 31 Proposta della Commissione, cit. In dottrina si è sottolineato che «la Commissione ha prestato la maggior parte delle sue attenzioni nei confronti dell'OPE (specie se concernente dati relativi alle operazioni e al contenuto), mentre ha tralasciato gli ordini di conservazione europei. Così facendo, ha dato vita per questi ultimi a un regime assai sbilanciato in favore delle esigenze repressive rispetto a quelle di tutela dei diritti fondamentali» (M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio, cit., p. 292).

[47] Dello stesso avviso J.H. Jeppesen-G. Nojeim, *Initial Observations*, cit., secondo cui «*Production Orders for subscriber information and access data can be issued in investigations of petty crimes and without judicial authorisation. This creates a risk that providers will be inundated with such demands*». Critica tale scelta normative anche M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio, cit., p. 293: «dato il valore fondamentale dei diritti degli indagati e imputati in gioco nella procedura in esame, non sembra, infatti, condivisibile la scelta di consentire alle autorità nazionali – salvo che per gli OPE concernenti *transnational* e *content data* – di utilizzare tali mezzi di ricerca della prova informativi per ogni tipologia di reati, senza alcun limite edittale di sorta stabilito *ex ante*».

sua successiva acquisizione.

In seguito all'emissione, l'OCE deve essere trasmesso al prestatore di servizi interessato che detiene i dati. A tal fine l'art. 8 della proposta prevede che si notifichi al *provider* uno *European Preservation Order Certificate* (EPOC-PR, certificato di conservazione europeo, Allegato II) con ogni mezzo che consenta di tracciarne per iscritto la trasmissione e garantisca al destinatario l'autenticità dello stesso. Così, ad esempio, è possibile trasmettere l'EPOC-PR tramite l'indirizzo di posta elettronica ordinaria (PEO) o di posta elettronica certificata (PEC) istituzionale dell'autorità competente, ovvero tramite una piattaforma dedicata o altri canali sicuri.

Dal canto suo, il *provider* è tenuto a conservare, senza indebito ritardo[48], per sessanta giorni i dati indicati nell'EPOC-PR e, trascorso tale periodo, non è più vincolato all'ordine, a meno che l'autorità di emissione confermi che è stata avviata una successiva richiesta di produzione: in tal caso il *provider* deve conservare i dati per tutto il tempo necessario nelle more dell'adozione di un OPE o di un OEI (art. 10, paragrafi 1 e 2, della proposta).

Vi sono però dei casi in cui il destinatario non può ottemperare all'ordine. Da un lato, vi sono le impossibilità materiali e le cause di forza maggiore, riferibili per lo più alla circostanza che il soggetto di cui si richiedono gli *e-data* non è cliente del *provider* (art. 10, paragrafo 5, della proposta); dall'altro, si situano talune mancanze dell'autorità di emissione che potrebbe emettere un ordine incompleto, contenente errori manifesti o informazioni insufficienti per eseguirlo (art. 10, paragrafo 4, della proposta).

Nel primo caso, qualora sia impossibile eseguire l'ordine per forza maggiore o impossibilità materiale, il *provider* interloquisce con l'autorità di emissione per mezzo dell'allegato III alla proposta, specificandone i motivi. Qualora l'autorità emittente ritenga esaustive le motivazioni del destinatario ritira l'ordine. In caso contrario, può attivare la procedura esecutiva di cui si parlerà *infra*.

Nel secondo caso, invece, la procedura è sottoposta a tempistiche più restrittive. Il *provider* deve comunicare il motivo di inottemperanza all'autorità emittente per mezzo dell'allegato III. Quest'ultima ha l'onere di integrare l'EPOC-PR entro cinque giorni dalla ricezione del richiamato allegato III, mentre il prestatore di servizi deve porsi nella condizione di poter ricevere i chiarimenti necessari per ottemperare all'obbligo.

Vi è, infine, una clausola di chiusura che facoltizza il *service provider* a non

[48] In dottrina si è evidenziato che «mentre il legislatore UE è stato particolarmente preciso nell'individuazione del termine d'esecuzione dell'ordine di produzione, non si comprende tale generica scelta rivolta all'ordine di conservazione che pure condivide con l'ordine di produzione la stessa *ratio*» (E. Colombo, *Ordini europei di produzione e di conservazione*, cit., p. 2725.

conservare le informazioni richieste "per altri motivi" (art. 10, paragrafo 6, della proposta). In tal caso deve fornire la comunicazione dell'allegato III all'autorità di emissione, che deve riesaminare l'ordine alla luce delle osservazioni ricevute ed eventualmente, nel caso in cui lo confermi, può richiedere l'intervento dell'autorità giudiziaria dello Stato di esecuzione, secondo la procedura di esecuzione di cui all'art. 14 della proposta.

Sul punto si può evidenziare come lo stato di forza maggiore, l'impossibilità materiale di trasmettere i dati, errori manifesti nella compilazione dell'ordine ovvero dati incompleti o insufficienti possano trovare una *ratio* giustificatrice nella quasi totale assenza di discrezionalità in capo al *service provider* nel disattendere l'ordine ricevuto e nella ristretta incidenza sui diritti del singolo. Al contrario, l'affidare ai SP la possibilità di non conservare le informazioni richieste per «altri motivi indicati nel modulo di cui all'allegato III» (art. 10, paragrafo 6) pare essere una clausola dalle maglie eccessivamente larghe che rischia di paralizzare il meccanismo e dare adito a potenziali comportamenti dilatori da parte degli operatori privati.

3.6. L'ordine europeo di produzione, per le sue caratteristiche maggiormente incisive sui diritti fondamentali, prevede presupposti applicativi maggiormente stringenti rispetto a quelli dettati per l'ordine di conservazione europeo.

Vi è, tuttavia, da fare una distinzione nell'ambito del presente strumento con riferimento ai dati che si vogliono ottenere, con tutele tanto maggiori quanto più il dato acquisito intacca i diritti fondamentali.

I dati relativi alle operazioni e al contenuto presuppongono il più alto livello di protezione, mentre quelli relativi agli abbonati e agli accessi non differiscono dalla procedura di emissione di un OCE (art. 5, paragrafo 4, lett. g) della proposta).

La dinamica degli OPE relativi a dati riguardanti operazioni e contenuto prevede che l'autorità competente ad emettere l'ordine sia un giudice, un organo giurisdizionale o un magistrato inquirente, ad eccezione dunque del pubblico ministero che potrà operare al più alla stregua di altra autorità competente che agisce nello Stato di emissione come autorità inquirente[49]. Così procedendo, tuttavia, l'ordine del pubblico ministero, al pari di quello della polizia giudiziaria, dovrà essere convalidato da un'autorità giurisdizionale, un giudice o un magistrato inquirente (art. 4, paragrafo 2, della proposta), che sarà considerata alla stregua dell'autorità di emissione dell'ordine (art. 4, paragrafo 4, della proposta).

In ragione del livello di intrusività che l'ordine di produzione ha sui diritti

[49] Ritiene eccepibile la proposta di rimettere al pubblico ministero l'adozione di un OPE relativo agli abbonati e agli accessi M. Daniele, *L'acquisizione delle prove dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1286.

fondamentali, primi fra tutti quelli alla inviolabilità del domicilio e alla riservatezza, la scelta di rimettere esclusivamente a un organo giurisdizionale la possibilità di emettere un OPE è certamente una scelta ragionevole e consente – almeno potenzialmente – di evitare che vengano emessi ordini di produzione privi dei necessari requisiti, tra cui il rispetto dei principi di proporzionalità e necessità.

Vi è però da domandarsi se anche per un OCE non sia opportuno prevedere che solo un giudice sia deputato alla sua emissione. La risposta non pare essere positiva, in quanto sarebbe irragionevole ritenere che il "congelamento" dei dati venga emesso dallo stesso organo che è il titolare del potere di disporne l'acquisizione. Al contrario, proprio la natura prodromica dell'OCE giustifica un intervento più rapido del pubblico ministero che successivamente potrà richiederne l'acquisizione.

Le ulteriori condizioni di emissione dell'OPE sono disciplinate all'art. 5 della proposta della Commissione.

Se per gli OCE, e anche per gli OPE concernenti dati relativi agli accessi, l'ordine può essere emesso per qualsiasi reato, gli OPE riguardanti dati relativi alle operazioni e al contenuto possono essere adottati esclusivamente per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno tre anni, in linea con quanto previsto in tema di OEI e di mandato di arresto europeo (MAE)[50] (art. 5, paragrafo 4, lett. a) della proposta)[51]. Inoltre, l'art 5, paragrafo 4, lett. b) della proposta della Commissione elenca una serie di reati per i quali lo strumento investigativo deve sempre essere disponibile in ragione del fatto della loro commissione in tutto o in parte per mezzo di un sistema di informazione[52], la quale tuttavia non rileva qualora si proceda per delitti riguardanti terrorismo, reclutamento o addestramento a fini di terrorismo, organizzazione di viaggi a fini terroristici e finanziamento del terrorismo, anche in forma tentata[53] (art. 5, paragrafo 4, lett. c) della proposta).

La scelta del legislatore europeo sembra essere giustificata dalla necessità di restringere l'ambito operativo dello strumento, al fine di rispettare il principio di proporzionalità e di evitare che il privato veda leso il proprio diritto alla riservatezza e/o alla segretezza delle comunicazioni in relazioni a fattispecie delittuose ritenute

[50] Decisione Quadro 2002/584 GAI del Consiglio, *relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri*, del 13 giugno 2002, in GUUE L 190 del 18 luglio 2018, pp. 1-18.

[51] Vi è da precisare che l'OEI e il MAE fanno riferimento non solo alle pene detentive, bensì anche alle misure di sicurezza.

[52] Trattasi dei reati di frode informativa (art. 3 DQ 2001/413/GAI); vendita di strumenti volti a commettere una frode informatica anche in forma di partecipazione, istigazione o tentativo, (artt. 4 e 5 DQ 2001/413/GA); reati sessuali nei confronti di minorenni e pornografia minorile (artt. da 3 a 7 direttiva 2011/93/UE); interferenze illecite in sistemi informatici, anche nella forma tentata (artt. da 3 a 8 direttiva 2013/40/UE).

[53] Artt. da 3 a 12 e 14 della direttiva 2017/541/UE del Parlamento europeo e del Consiglio, *sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAIdel Consiglio e che modifica la decisione 2005/671/GAI del Consiglio*, del 15 marzo 2017, in GUUE L 88 del 31 marzo 2017, pp. 6-21.

prive – in un un'ottica *ex ante* – di una certa soglia di gravità.

Sotto questo profilo la proposta della Commissione effettua una scelta differente da quella adottata in tema di OEI e di MAE (e non solo[54]), i quali elencano una serie di 32 (gravi) reati per cui i citati strumenti devono essere sempre disponibili (indipendentemente dal requisito della doppia incriminazione) qualora siano puniti nello stato di emissione con una pena o una misura di sicurezza detentive della durata massima non inferiori a tre anni.

Sarebbe forse maggiormente opportuno propendere per un'armonia di sistema e adeguare la proposta agli strumenti di cooperazione giudiziaria vigenti. Così operando il principio di proporzionalità sarebbe rispettato – in virtù del consolidato orientamento creatosi negli ultimi vent'anni –, in quanto, da un lato, si prevede che la pena detentiva massima deve essere non inferiore a tre anni e, dall'altro, l'indicazione delle 32 fattispecie delittuose comprendono reati di elevato disvalore sociale, tra i quali sono compresi i delitti di criminalità informatica, di terrorismo e sessuali richiamati dalla proposta della Commissione.

I dati richiesti relativi alle operazioni e al contenuto possono essere oggetto di immunità o privilegi – si pensi al caso in cui si proceda nei confronti di agenti diplomatici o di professionisti vincolati al segreto professionale – ovvero incidere su interessi fondamentali dello Stato, tra cui si possono annoverare la sicurezza pubblica o la difesa nazionale. Se i privilegi e le immunità riguardano un residente nello Stato di emissione, *nulla quaestio*: dovranno essere valutati ai sensi della normativa nazionale interna. Nel caso in cui, invece, le immunità e i privilegi concernano un soggetto residente in un altro Paese, ovvero si controverta su interessi fondamentali dello Stato, l'art. 5, paragrafo 7, della proposta impone allo Stato di emissione di consultarsi preventivamente con le autorità competenti dello Stato di esecuzione, direttamente ovvero tramite Eurojust o la Rete Giudiziaria Europea. Se, dalla consultazione, emerge che i dati richiesti sono coperti da immunità o privilegi, ovvero vanno a minare la sicurezza pubblica e la difesa nazionale dello Stato di esecuzione, l'Autorità di emissione non può emettere l'OPE.

Vi è però da domandarsi cosa accada nel caso in cui le immunità e i privilegi vengano scoperti successivamente alla trasmissione dei dati allo Stato di emissione. La

[54] Si pensi, ancora a titolo esemplificativo, alla DQ 2008/909/GAI relativa all'applicazione del principio del reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale, ai fini della loro esecuzione nell'Unione europea; alla DQ 2009/947/GAI relativa all'applicazione del principio del reciproco riconoscimento alle sentenze e alle decisioni di sospensione condizionale in vista della sorveglianza delle misure di sospensione condizionale e delle sanzioni sostitutive; alla DQ 2008/829/GAI sull'applicazione tra gli Stati membri dell'Unione europea del principio del reciproco riconoscimento alle decisioni sulle misure alternative alla detenzione cautelare; al regolamento 2018/1805/UE relativo al riconoscimento reciproco dei provvedimenti di congelamento e di confisca.

proposta sembra silente sul punto e non pare che si possa fare riferimento a una causa di inutilizzabilità espressa della proposta stessa. Eventualmente si può ritenere che siano le legislazioni nazionali a farsi carico del problema, con la conseguente possibilità di rinvenire un quadro normativo frammentario che si pone in contrasto con la *ratio* di unificazione che è alla base della proposta. Si anticipa sin d'ora, però, che l'orientamento generale del Consiglio dell'UE – qualora recepito – ha posto rimedio al problema con l'introduzione di una causa di inutilizzabilità specifica postuma.

In seguito all'emissione, l'OPE, al pari dell'OCE e con le stesse modalità, deve essere trasmesso al prestatore di servizi interessato che detiene le *e-evidence*.

Non appena ricevuto l'EPOC, il destinatario è tenuto a trasmettere i dati richiesti dall'autorità di emissione entro 10 giorni dalla ricezione, a meno che quest'ultima non indichi i motivi di una divulgazione anticipata, la quale, in caso di emergenza, può obbligare a traferire i dati entro sei ore dalla notifica dell'ordine (art. 9, paragrafi 1 e 2, della proposta)[55]. Un lasso temporale, quello di sei ore, che rischia di rivelarsi fin troppo breve per rispondere alle richieste dell'autorità, in particolar modo nelle realtà meno strutturate che potrebbero non essere in grado di rispettare le tempistiche imposte.

Nel caso in cui, invece, il destinatario ritenga che, sulla base delle indicazioni contenuto nell'EPOC, risulti che l'ordine violi manifestamente i diritti fondamentali o che sia manifestamente arbitrario, deve notiziare per mezzo dell'allegato III non solo lo Stato di emissione, bensì anche quello di esecuzione competente nel proprio Stato. A questo punto l'autorità di esecuzione può interloquire con l'autorità di emissione, direttamente ovvero tramite Eurojust o la Rete Giudiziaria Europea, e confermare o respingere l'ordine.

La clausola che rimette la tutela dei diritti e interessi fondamentali a soggettivi privati, è stata salutata con favore da parte della dottrina, la quale ha sottolineato che a differenza di altri contesti «in cui la scelta di affidare a operatori privati (quali i prestatori di servizi digitali) l'*enforcement* degli strumenti di tutela pare sollevare criticità, in questo specifico ambito l'opzione racchiusa nella proposta di regolamento *e-Evidence* si ritiene condivisibile e rispondente alla migliore tutela degli interessi in gioco»[56]. Un intervento preventivo dell'autorità giudiziaria dello Stato di esecuzione, invero, vanificherebbe i «benefici connessi alla disintermediazione»[57] e sacrificherebbe

[55] Con riferimento alle tempistiche in dottrina si è osservato che «il regolamento e-Evidence pare indulgere talvolta in un eccesso di ottimismo con riferimento alla tempistica per dare luogo alle procedure di esecuzione o di opposizione all'esecuzione di ordini europei di conservazione o produzione» (O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence, cit., p. 6).

[56] O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence, cit., p. 7.

[57] O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence, cit., p. 7.

la funzionalità della procedura in esame[58].

Rinviando a quanto si dirà *infra*, si può qui anticipare che la disintermediazione totale, in un'ottica che consenta una maggiore tutela dei diritti fondamentali ma che garantisca al contempo un procedimento rapido, potrebbe essere contemperata dalla notifica allo Stato di residenza della persona i cui dati sono richiesti. Invero, le situazioni che si possono creare con l'emissione di un ordine sono tre: il soggetto i cui dati sono richiesti si trova nel territorio dello Stato di emissione (ed è il caso statisticamente più frequente); il soggetto i cui dati sono richiesti si trova nel territorio dello Stato di esecuzione; il soggetto i cui dati sono richiesti si trova nel territorio di uno Stato membro differente dai primi due. Nel primo caso *nulla quaestio*: i diritti fondamentali sono garantiti dallo Stato emittente, nel quale possono essere proposti gli opportuni mezzi di gravame. Nel secondo e nel terzo caso, invece, la tutela dei diritti del singolo è affidata allo Stato in cui il soggetto si trova (sia esso nello Stato di esecuzione o in altro Stato) e per tale motivo potrebbe essere prevista la notifica dell'ordine allo Stato di residenza del soggetto i cui dati vengono richiesti, il quale sarebbe tenuto ad effettuare il vaglio di manifesta violazione dei diritti fondamentali o di manifesta arbitrarietà dell'ordine oggi richiesta ai *service provider*. Lo stato notificato, tuttavia, non dovrebbe riconoscere l'ordine, ma al più opporvisi se si verificano le condizioni di violazione dei diritti appena citate. Inoltre, al fine di non frustrare "l'appetibilità" e l'efficacia dello strumento, in attesa di una eventuale opposizione dello stato notificato o di un suo silenzio-assenso, il SP dovrebbe essere tenuto a conservare i dati nel caso in cui l'esito della stessa fosse positivo.

3.7. Come visto, vi possono essere delle situazioni in cui il prestatore di servizi non ottempera all'ordine (EPOC o EPOC-PR) ricevuto. Se l'autorità di emissione ritiene esaustive le giustificazioni del destinatario ritira l'ordine e il procedimento è interrotto. Al contrario, se il *provider* non fornisce alcuna motivazione, ovvero se

[58] Vi è, tuttavia, da segnalare una dottrina di avviso differente secondo cui, nella proposta in esame, vi è un'evidente «difficoltà derivante dal fatto di attribuire al prestatore di servizi il compito di valutare se l'ordine ricevuto si ponga in contrasto con gli obblighi derivanti dalla Carta dei diritti fondamentali dell'Unione europea e dall'articolo 6 del Trattato sull'Unione europea, dunque di richiedere a un privato di operare al fine della tutela dei diritti fondamentali come se fosse un'autorità giudiziaria» (A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea*, op. cit., p. 14). Dello stesso avviso M. Daniele, *L'acquisizione delle prove dai* service provider, op. cit., p. 1290, secondo cui «ci sono, tuttavia, forti dubbi che un tale complesso meccanismo possa sortire i suoi effetti, e ciò per una ragione connessa alla stessa essenza dei *provider*: i quali, a causa della loro natura privatistica e della conseguente – e legittima – esigenza di proteggere i loro interessi, non potrebbero mai agire come organi pubblici in posizione di imparzialità, di per sé del tutto indifferenti all'esito del vaglio. Per quanto possano avere a cuore la *privacy* dei loro utenti, la loro condotta sarebbe condizionata dalla comprensibile necessità di mantenere buoni rapporti con gli Stati in cui esercitano la loro attività economica. Il rischio, poi, che, rifiutandosi di eseguire gli ordini di conservazione o produzione dei dati, siano esposti a sanzioni, inevitabilmente falserebbe le loro valutazioni».

quest'ultima è fornita ma è ritenuta non soddisfacente, l'autorità di emissione può attivare la procedura di "esecuzione coatta"[59] prevista dall'art. 14 della proposta della Commissione e adire l'autorità dello Stato di esecuzione.

Adita l'autorità di esecuzione, questa è tenuta a riconoscere l'ordine al più tardi entro cinque giorni e a ingiungere al destinatario di darvi seguito entro un termine indicato, informandolo delle sanzioni conseguenti all'inottemperanza, nonché della possibilità di invocare uno dei motivi di non riconoscimento tassativamente indicati (art. 14, paragrafo 3, della proposta)[60].

Questi ultimi sono gli stessi che possono essere invocati da parte dell'autorità di esecuzione, la quale può non riconoscere gli ordini altresì nei casi in cui i dati siano coperti da immunità o privilegi, ovvero ancora se la loro divulgazione possa compromettere un interesse fondamentale dello Stato (art. 14, paragrafo 2, della proposta).

Se vi è opposizione del destinatario (art. 14, paragrafo 6, della proposta), l'autorità di esecuzione decide se eseguire o respingere l'ordine sulla base del compendio conoscitivo a propria disposizione e delle informazioni ricevute dal *provider*. Tuttavia, nel caso in cui l'autorità di esecuzione sia determinata a non eseguire o non riconoscere l'ordine, questa è tenuta a consultare l'autorità di emissione con ogni mezzo appropriato, eventualmente richiedendo informazioni aggiuntive. Dalla sua parte, l'autorità di emissione fornisce i chiarimenti necessari entro cinque giorni (art. 14, paragrafo 7, della proposta). Così disponendo, la proposta si allinea a

[59] L'art. 14 della proposta della Commissione ha come rubrica «procedura di esecuzione». In realtà sembra più corretto riferirsi a una esecuzione coatta, atteso che la procedura esecutiva è già prevista sia per l'OCE sia per l'OPE.

[60] I motivi di non riconoscimento, che sono al quanto differenti da quelli previsti in tema di OEI e MAE (v. sul punto S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., p. 175), sono per lo più di natura formale e riguardano: 1) un ordine proveniente da un'autorità incompetente; 2) nel solo caso dell'OPE, un ordine che non rientra nelle categorie di reati tassativamente indicate; 3) l'impossibilità materiale di ottemperare all'ordine da parte del destinatario; 4) un ordine riferito a dati non conservati dal prestatore di servizi; 5) un servizio che esula dall'ambito di applicazione della proposta di regolamento; 6) una violazione manifesta, desumibile dall'EPOC o dall'EPOC-PR, dei diritti fondamentali previsti dalla Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE o Carta di Nizza).
Si può notare come la tecnica normativa del richiamo, operato dall'art. 14, paragrafo 2, all'art. 14, paragrafi 4 e 5, della proposta sconti almeno un'imprecisione. Invero, il riferimento alle «sole informazioni contenute nell'EPOC» o nell'EPOC-PR può trovare applicazione esclusivamente con riferimento al *service provider*, dal momento che all'autorità di esecuzione devono essere trasmessi non solo l'EPOC (o l'EPOC-PR), bensì anche l'OPE (o l'OCE) e ogni altro elemento utile. In altri termini, l'autorità di esecuzione ha a disposizione un compendio conoscitivo ben superiore a quello fornito al prestatore di servizi, dal momento che gli OPE e gli OCE indicano le ragioni di necessità e proporzionalità, che sono escluse dai relativi certificati, e permettono un sindacato più approfondito rispetto a quello fornito al prestatore di servizi.

quanto previsto dall'art. 11, paragrafo 4, direttiva OEI, il quale analogamente prevede la procedura di consultazione preventiva nel caso in cui l'autorità di esecuzione sia indirizzata a non eseguire l'ordine. Inoltre, si può immaginare che anche in tema di ordini di produzione e conservazione si incardinerà la prassi di ricorrere a consultazioni informali tra autorità giudiziarie – quali telefonate ed e-mail – che consentono di raggiungere il medesimo risultato con maggiore celerità in un clima di cortesia internazionale.

La decisione finale dell'autorità di esecuzione è notificata sia al *service provider* sia all'autorità di emissione. Nel caso di riconoscimento dell'ordine e di ottenimento dei dati, l'autorità di esecuzione, a cui gli stessi sono trasmessi, se non si avvede in questa fase che gli stessi sono coperti da privilegi o immunità ovvero che possono ledere gli interessi fondamentali dello Stato, deve a sua volta trasferirli all'autorità di emissione. L'interlocuzione diretta pubblico/privato interstatale è, infatti, venuta meno in seguito all'attivazione della procedura di esecuzione di cui all'art. 14 della Proposta.

Infine, può ancora accadere che, nonostante l'autorità giudiziaria del proprio Stato abbia confermato l'ordine, il destinatario non adempia. In simili evenienze, al *provider* può essere irrogata una sanzione pecuniaria conformemente al diritto interno (artt. 13 e 14 della proposta), ma gli interessi investigativi dell'autorità di emissione rimarranno insoddisfatti.

Il rimettere la sanzione pecuniaria alla disciplina dello Stato membro di esecuzione dimostra l'atteggiamento "direttivo" che il regolamento assume in taluni punti e potrebbe creare disparità di trattamento e operazioni di *forum shopping*. Invero, se un *provider* non fosse intenzionato a collaborare con le autorità per difendere la riservatezza dei dati dei propri clienti, o se volesse scongiurare il rischio di sanzioni pecuniarie elevate in caso di inottemperanza "colposa", allora ben potrebbe scegliere di stabilirsi (o trasferire la propria sede se già stabilito) nello Stato membro in cui le sanzioni pecuniarie sono le più miti. A ciò si aggiunga che vi può essere il rischio che gli Stati possano manovrare "al ribasso" le proprie scelte in merito alle sanzioni da irrogare (che comunque dovrebbero rimanere effettive, proporzionate e dissuasiva), al fine di essere più competitivi e attrarre un maggior numero di SP sul proprio territorio. Pertanto sarebbe opportuno prevedere un meccanismo che elimini alla radice, o comunque attenui quanto più possibile, il rischio di *forum shopping*.

In ogni caso, se i dati richiesti sono indispensabili ai fini delle indagini, l'autorità procedente potrà comunque ottenerli per il tramite di un OEI o di una rogatoria internazionale, sebbene le tempistiche richieste per questi ultimi procedimenti rischino di compromettere definitivamente l'acquisizione del dato che, nelle more, potrebbe venire cancellato definitivamente o modificato.

3.8. La proposta disciplina il caso in cui un ordine europeo di produzione (ma non un ordine europeo di conservazione) violi i diritti fondamentali o gli interessi fondamentali (sicurezza e difesa nazionali) di un Paese terzo (art. 15 della proposta), ovvero si ponga in contrasto con la legislazione di quest'ultimo per altri motivi (art. 16 della proposta).

Qualora si avveda di ciò, il destinatario deve informare l'autorità di emissione e fornire una serie di indicazioni al fine di consentire a quest'ultima di riesaminare l'OPE. In particolare, l'informazione contiene l'esposizione del diritto del Paese terzo, la sua applicabilità al caso di specie e la natura dell'obbligo contrastante.

Nel caso in cui intenda confermare l'ordine, perché ritiene che il diritto del Paese terzo non sia applicabile, ovvero che l'ordine non si ponga in contrasto con i diritti fondamentali o gli interessi di tale Stato, l'autorità di emissione ne chiede il riesame da parte dell'organo giurisdizionale competente del proprio Stato membro. Ci si può domandare, tuttavia, quale sia l'organo giurisdizionale competente se l'ordine è già stato emesso, per l'appunto, da un organo giurisdizionale, direttamente o in sede di convalida: potrebbe essere lo stesso organo (anche persona fisica) o potrebbe esservi un inedito deferimento *ex officio* ad altra sezione, all'organo superiore o al presidente dello stesso? La risposta, certo non agevole, non può che essere lasciata alle normative nazionali che dovranno adattare il proprio sistema processuale interno alla luce del regolamento.

In ogni caso, il riesame dell'organo giurisdizionale verte su un duplice aspetto che consiste nella verifica dell'applicabilità del diritto alieno e, in caso affermativo, nella valutazione circa la compatibilità dello stesso con la divulgazione dei dati richiesti.

A questo punto la procedura varia a seconda che il motivo di contrasto sia basato su un'incompatibilità con i diritti fondamentali di un soggetto o gli interessi fondamentali dello Stato terzo ovvero sia fondato su altri motivi.

Nel primo caso, l'organo giurisdizionale adito in "sede di riesame" da parte dell'autorità emittente deve vagliare se il diritto del Paese terzo intenda manifestamente tutelare interessi differenti dai diritti e interessi fondamentali ovvero proteggere attività illecite (art. 15, paragrafo 4, della proposta). Orbene, per quanto il principio *iura novit curia* sia stato ritenuto applicabile, almeno dalla giurisprudenza italiana[61], anche alla conoscenza di una legislazione straniera e alla sua interpretazione, affidare l'indagine circa l'intenzione di una legislazione di un Paese a un giudice di uno Stato diverso da quello della legislazione stessa, magari anche con valori diametralmente opposti, pare essere un'operazione estremamente delicata e

[61] V *ex multis*, Cass. civ, Sez. II, 24 ottobre 2019, n. 27365.

difficoltosa. E ciò a maggior ragione se si ritiene che indagare l'intenzione di una normativa è operazione alquanto complessa già nello stesso ordinamento in cui deve essere applicata.

In ogni caso, se il giudice ritiene che non vi sia alcun contrasto e intenda confermare l'ordine, ne informa l'autorità di emissione e il destinatario, affinché quest'ultimo proceda a ottemperare (art. 15, paragrafo 8, della proposta).

Nel caso in cui, invece, l'organo giurisdizionale competente per il "riesame" ravvisi uno dei motivi di contrasto con il diritto del Paese terzo, ne informa immediatamente le autorità centrali, trasmettendo tutte le «pertinenti informazioni fattuali e giuridiche relative al caso, compresa la propria valutazione, fissando un termine di 15 giorni per rispondere» (art. 15, paragrafo 5, della proposta). A questo punto si apre una triplice via: 1) l'autorità centrale si oppone all'esecuzione dell'ordine e il procedimento si arresta; 2) sebbene non espressamente previsto, l'autorità centrale non si oppone all'esecuzione; 3) l'autorità centrale non si attiva né in un senso né nell'altro, rimanendo silente. In quest'ultima situazione si apre un "procedimento di messa in mora" per cui l'autorità centrale dello Stato terzo è sollecitata a rispondere entro 5 giorni, con l'avvertimento che l'inattività sarà considerata come un silenzio assenso e l'ordine verrà confermato (art. 15, paragrafo 6, della proposta).

In caso di non opposizione, espressa o tacita, l'organo giurisdizionale competente per il riesame conferma l'ordine e informa l'autorità di emissione e il destinatario, affinché quest'ultimo proceda a ottemperare (art. 15, paragrafo 8, della proposta).

Nel secondo caso, qualora l'incompatibilità con la normativa dello Stato terzo sia fondata su motivi diversi dai diritti o interessi fondamentali, la procedura segue un *iter* differente.

L'organo giurisdizionale, in caso di incompatibilità che vieta la divulgazione dei dati, può decidere di confermare o ritirare l'ordine tenendo a seguito di un giudizio di bilanciamento tra cinque diversi fattori [62], comunicando la propria decisione all'autorità di emissione.

Si può notare, dunque, come questo secondo meccanismo di opposizione, non incidendo direttamente sui diritti fondamentali dell'individuo ovvero sulla sicurezza pubblica o difesa nazionale, è disegnato con una veste più snella rispetto al primo e

[62] I fattori da considerare nel bilanciamento sono: 1) l'interesse tutelato dal diritto del Paese terzo, anche in relazione all'interesse dello stesso alla divulgazione dei dati; 2) il grado di collegamento del procedimento penale per il quale l'ordine è stato emesso con una delle due giurisdizioni; 3) il grado di collegamento tra il prestatore di servizi e lo Stato terzo; 4) l'interesse dello Stato di emissione a ottenere le prove, sulla base dell'importanza di acquisire le stesse rapidamente e della gravità del reato; 5) le possibili conseguenze per il destinatario o il prestatore di servizi in caso di ottemperanza all'OPE, comprese le sanzioni in cui può incorrere (art. 16, paragrafo 5, della proposta).

non prevede l'intervento dell'autorità centrale dello Stato terzo. Una scelta di politica legislativa che pare essere in armonia con l'intelaiatura della proposta, che fa corrispondere una maggiore tutela nel momento in cui la lesione dei diritti e interessi fondamentali è più alta, sebbene rimangano dubbi circa l'opportunità di rimettere a un giudice di uno Stato membro l'indagine circa le finalità di una legislazione di uno Stato terzo.

Inoltre, così disponendo vi può essere il rischio di un'intromissione di uno Stato membro dell'UE nella sovranità di un Paese extra-comunitario che potrebbe quantomeno potenzialmente creare conflitti di giurisdizione tra i due. Sarebbe quindi, forse, auspicabile che anche in questa seconda ipotesi vi sia un coinvolgimento dell'Autorità centrale del Paese terzo prima della trasmissione dei dati allo Stato richiedente, eventualmente garantendo l'immodificabilità degli stessi con la loro conservazione in attesa della decisione.

Vi è tuttavia da considerare che il gravoso onere incombente sui *service provider*, i quali sembrerebbero essere tenuti a conoscere la legislazione applicabile di qualsiasi Paese terzo e a valutare se l'ordine si ponga in contrasto con la stessa, al fine di garantirne gli interessi politici.

Sul punto ha preso posizione la Corte di Giustizia che, nella sentenza *Schrems II* sul c.d. *Privacy Shield*, sembra effettivamente imporre ai SP di verificare «se il diritto del paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati»[63], con la conseguenza che «il titolare del trattamento stabilito nell'Unione e il destinatario del trasferimento di dati personali sono tenuti a verificare, preliminarmente, il rispetto, nel paese terzo interessato, del livello di protezione richiesto dal diritto dell'Unione»[64].

Se la citata giurisprudenza dovesse trovare applicazione anche in relazione alla proposta, ai *provider* verrebbe richiesto il compito quasi impossibile di conoscere la legislazione di un numero potenzialmente infinito di Stati extraeuropei, incombente che probabilmente nemmeno la Commissione europea potrebbe essere in grado di svolgere[65]. E ciò potrebbe condurre a un eventuale duplice paradosso qualora il *provider* abbia a confrontarsi con i diritti in gioco in un Paese terzo: o, precauzionalmente, rifiuta ogni proposta, rimettendo all'autorità giudiziaria emittente un più severo vaglio sulla tutela dei diritti coinvolti e dilatando i tempi di esecuzione; o esegue l'ordine, accelerando la procedura ma rischiando che non siano stati garantiti

[63] CGUE, Grande Sezione, 16 luglio 2020, C-311/18, *Schrems II*, §134.

[64] CGUE, Grande Sezione, 16 luglio 2020, C-311/18, *Schrems II*, §142.

[65] T. Christakis, *After Schrems II: Uncertainties on the Legal Basis for Data Transfer and Constitutional Implications for Europe*, in *www.europeanlawblog.eu*, 21 luglio 2020.

i diritti individuali.

Per esemplificare, si può pensare a un OPE, emesso da un'autorità italiana nei confronti di un *provider* stabilito in Spagna, per reati commessi da un cittadino e residente brasiliano durante la sua permanenza in Italia.

Sembra chiaro che non è opportuno gravare il SP di verificare se l'ordine emesso dall'Italia sia conforme alla disciplina brasiliana, sicché sarebbe forse maggiormente auspicabile, in simili situazioni, che vi sia una notifica anche allo Stato in cui ha sede il *provider*¸ affinché sia l'autorità giudiziaria a valutare la conformità o meno della disciplina, eventualmente richiedendo l'ausilio del Paese terzo interessato. Durante questa procedura, al fine di non vanificare l'acquisizione del dato, che a causa delle tempistiche potrebbe venire modificato o cancellato, il *provider* dovrebbe essere tenuto a conservarlo – senza produrlo – sino a una delibazione positiva da parte dell'autorità giudiziaria dello Stato richiesto.

3.9. Il diritto a un ricorso effettivo, in pubblica udienza, davanti a un giudice terzo e imparziale, precostituito per legge, è una garanzia elevata a diritto fondamentale dell'Unione Europea dall'art. 47 della Carta di Nizza.

L'art. 17 della proposta della Commissione, rubricata «ricorso effettivo», dà attuazione, almeno in parte, alla normativa sovraordinata e prevede che gli indagati, gli imputati e le persone i cui dati sono stati ottenuti hanno diritto a un ricorso giurisdizionale effettivo nello Stato di emissione, in conformità al diritto nazionale, per contestare tanto motivi di legittimità quanto motivi di merito dell'ordine di produzione europeo. Non è previsto, invece, alcun rimedio se l'illegittimità dell'ordine verte sugli OCE, dal momento che il regolamento sembra ritenere tale strumento non sufficientemente invasivo dei diritti fondamentali, primo fra tutti quello alla riservatezza. Una soluzione, questa, che può porgere il fianco a numerose critiche poiché se è vero che l'invasione della sfera fondamentale dell'individuo è minore rispetto a quella di un OPE, comunque non si può sostenere che sia del tutto assente e non meritevole di tutela[66].

Il ricorso è presentato dinanzi l'autorità giudiziaria procedente se proviene da un indagato o un imputato, mentre gli altri soggetti dovranno adire l'autorità (civile)

[66] In dottrina, dello stesso avviso, R.M. Geraci, *La circolazione transfrontaliera*, cit., p. 1360, secondo cui con riferimento agli OCE «la proposta di regolamento stabilisce una disciplina tutt'altro che garantista, connotata dalla generale attivabilità (non essendo previsti limiti edittali per la loro adozione) e dalla pressoché nulla contestabilità (non essendo contemplata la possibilità di riesame ed il diritto ad un ricorso effettivo, validi solo rispetto all'ordine europeo di produzione), in evidente spregio peraltro quanto previsto in via generale dall'art. 47, par. 1 della Carta di Nizza». Nello stesso senso M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio, cit., p. 293; E. Sellier-A. Weyembergh, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, Brussels 2018, p. 43.

al di fuori dell'ambito del processo penale e, quanto a termini e modalità, seguirà le procedure previste dal diritto interno in casi analoghi. Un doppio binario basato sullo *status* di imputato/indagato e altri soggetti non sembra del tutto condivisibile, in quanto vi sarebbero strumenti di tutela alquanto differenti per posizioni soggettive che meritano la medesima attenzione.

Sarebbe forse maggiormente opportuno prevedere – analogamente al riesame in tema di sequestro probatorio del terzo coinvolto previsto nel nostro ordinamento – che sia l'autorità procedente a giudicare tanto sulla posizione degli imputati/indagati quanto di quella degli altri soggetti attinti dall'ordine.

Ancora una volta, inoltre, si può notare la commistione tra una direttiva e un regolamento, in quanto la proposta della Commissione affida ai rimedi giurisdizionali interni dei singoli Stati membri le doglianze circa l'illegittimità degli ordini (*rectius*: del solo OPE), con il rischio che – analogamente a quanto accaduto in tema di OEI – taluni Stati membri introducano un rimedio *ad hoc* (Italia, Austria e in parte Germania) e talaltri si affidino a quelli già esistenti (Croazia, Portogallo, Slovenia).

Preso atto delle difficoltà che la proposta della Commissione sta incontrando nell'*iter* di formazione del regolamento, è decisamente prematuro provare a sostenere la necessità di un'uniformazione dei rimedi giurisdizionali sul tema in tutta l'Unione Europea. Tuttavia, se la cooperazione giudiziaria in materia penale evolverà con la rapidità degli ultimi vent'anni, un flebile auspicio che strumenti comuni siano giudicati anche secondo procedure comuni (o addirittura con corti comuni) nei prossimi decenni vi può essere.

4. Dal 17 aprile 2018 al 20 novembre dello stesso anno il Consiglio, sotto le presidenze bulgara e austriaca, si è riunito dodici volte per discutere proposte migliorative della bozza della Commissione ed è giunto, il 30 novembre 2019, ad elaborare il testo di base assunto come orientamento generale nella sessione del Consiglio GAI tenuta il 6 e 7 dicembre 2018 (orientamento generale)[67].

In primo luogo, l'orientamento generale si fa pregevolmente carico della problematica del *ne bis in idem* processuale internazionale al considerando 12 *bis* imponendo di non procedere all'emissione dell'ordine in situazioni di contemporanea pendenza di due procedimenti penali per la medesima vicenda. Qualora vi sia il dubbio sulla sussistenza del parallelo procedimento penale, viene previsto un obbligo di

[67] Orientamento generale del Consiglio sulla proposta di *regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 6 e 7 dicembre 2018, 2018/0108(COD). Per un primo commento all'orientamento generale v. T. Christakis, *"Big Divergence of Opinions on e-Evidence in the EU Council: a Proposal in order to Disentangle the Notification Knot*, in *www.crossborderdataforum.org*, 22 ottobre 2018; T. Christakis, *E-Evidence in the EU Council: the Key Issure of when One Member State can Review the Request from Another*, in *www.crossborderdataforum.org*, 01 ottobre 2018.

consultazione dello Stato membro interessato al fine di dissipare ogni incertezza. In tal modo il Consiglio tenta di allineare la proposta a quanto già previsto dalla direttiva 2014/41/UE che prevede quale motivo di non riconoscimento dell'ordine la contemporanea pendenza di due procedimenti penali per il medesimo fatto. Tuttavia, la tematica del *ne bis in idem* è trattata esclusivamente nel considerando 12 *bis* – che richiedere di ricorrere alle procedure di risoluzione dei conflitti previste dalla decisione quadro 2009/948/GAI – ma non trova alcun riflesso nella parte prescrittiva, con la conseguenza che pare non esservi alcun rimedio nel caso in cui vi sia una violazione del divieto di secondo giudizio. Si è in presenza, in altri termini, di una disposizione meramente esortativa.

In ogni caso, è altresì possibile che lo Stato di emissione non si avveda della pendenza di un procedimento parallelo, dal momento che solitamente è il difensore dell'indagato a portare a conoscenza delle autorità la presenza di un altro procedimento, ma nella fase delle indagini preliminari, caratterizzata da tendenziale segretezza, l'interessato può non essere stato messo ancora nelle condizioni di esercitare compiutamente il diritto di difesa. Pare difficilmente ipotizzabile che il *service provider* possa supplire a una mancanza dello Stato di emissione, stante la sua natura privata e l'impossibilità di accedere ai registri contenenti le notizie di reato e i procedimenti penali. Sarebbe, dunque, opportuno prevedere una sanzione di inutilizzabilità dei dati raccolti nel caso in cui, a seguito della *discovery*, vi siano evidenze di una violazione del *ne bis in idem* processuale.

Muta anche la definizione di prestatore di servizi. Viene, infatti, precisato che il regolamento dovrebbe essere applicabile ai *service provider* che offrono la possibilità agli utenti di comunicare tra loro oppure che trattano dati per conto degli utenti (art. 2, paragrafo 3, dell'ordinamento generale). Più precisamente, si escludono dal novero dei prestatori di servizi, oltre ai servizi finanziari, coloro che offrono la possibilità agli utenti di comunicare esclusivamente con il prestatore di servizi e non tra loro, che non offrono la possibilità di tracciare o conservare dati ovvero questi ultimi servizi non sono parte essenziale dell'attività svolta[68].

Apprezzabile è anche l'idea di prevedere l'utilizzabilità degli ordini non solo per l'identificazione dell'indagato o imputato ovvero per l'acquisizione di materiale probatorio, ma anche per l'individuazione del soggetto condannato, non in contumacia[69], latitante che deve scontare l'esecuzione di una pena o di una misura di sicurezza privative della libertà della durata di almeno 4 mesi (artt. 3, paragrafo 2, 5

[68] Considerando 16 Orientamento generale, cit.

[69] L'esclusione dei soggetti condannati in contumacia è giustificata «dal momento che il diritto nazionale degli Stati membri in materia di sentenze contumaciali varia notevolmente all'interno dell'Unione europea» (considerando 24 *ter* Orientamento generale, cit.).

paragrafo 3, e 6 paragrafo 2, dell'orientamento generale).

Si può notare come manchi l'espressa previsione dell'esecuzione nei confronti del latitante di una misura cautelare custodiale, forse giustificata dal fatto che la custodia cautelare in carcere, per sua natura, non ha una durata determinata. Non si può, infatti, utilizzare quale parametro di riferimento una durata minima della misura cautelare, dal momento che non si può prevedere se la stessa possa durare un giorno, una settimana o quattro mesi. Al più, al fine di consentire di utilizzare lo strumento in esame per la ricerca del latitante che si sottrae a una misura cautelare, si potrebbe fare riferimento al limite edittale minimo e massimo della pena detentiva per il reato per il quale si procede: così si eviterebbe l'*empasse* della durata della detenzione e si garantirebbe in ogni caso l'utilizzo del mezzo di ricerca della prova per reati di una certa gravità.

Anche la procedura di emissione degli ordini è oggetto di talune modifiche.

In primo luogo, si prevede che in casi di «urgenza debitamente giustificati» (art. 4, paragrafo 5,) è consentita la trasmissione dell'EPOC-PR e dell'EPOC riguardante i dati relativi agli accessi e agli abbonati al destinatario in assenza della citata convalida, che dovrà comunque essere richiesta *ex post* entro 48 ore. Se viene rifiutata, l'autorità di emissione deve revocare l'ordine ed eliminare gli eventuali dati che *medio tempore* le sono stati trasmessi. Non viene prevista, invece, la procedura di emergenza nelle situazioni maggiormente incisive sui diritti fondamentali riguardanti l'acquisizione di dati relativi agli abbonati e al contenuto, al fine di garantire il rispetto del principio di proporzionalità. Tuttavia, così disponendo vi potrebbe essere il rischio che i dati ricercati subiscano alterazioni o cancellazioni. Pertanto, una soluzione intermedia che garantisca al contempo la tutela dei diritti fondamentali e le esigenze di celerità del procedimento potrebbe essere quella di affidare al pubblico ministero – autorità non competente ai fini dell'emissione di un OPE – l'adozione di un ordine in via d'urgenza. Il pubblico ministero, infatti, fornirebbe una garanzia maggiore rispetto a quella offerta dalla polizia giudiziaria, sebbene inferiore a quella di un giudice, ma un controllo giurisdizionale sarebbe in ogni caso ripreso mediante un controllo postumo sull'operato del PM.

In relazione al solo ordine di produzione europeo per dati concernenti le operazioni, se gli *e-data* richiesti riguardano una persona non residente nel territorio dello Stato di emissione e vi è il dubbio che possano essere oggetto di protezione nello Stato di esecuzione – perché coperti da immunità, privilegi, norme a tutela della libertà della stampa, o che possono minare i diritti fondamentali, la sicurezza e la difesa nazionali – è aggiunta una procedura preventiva di consultazione con lo Stato di esecuzione (art. 5, paragrafo 7, dell'orientamento generale). Se viene confermato il dubbio, l'autorità di emissione deve tenere conto delle circostanze come se fossero

presenti nel proprio diritto interno, evitando di adottare l'ordine o adattandolo alle caratteristiche del caso concreto.

Per di più, è espressamente prevista la revoca delle immunità o dei privilegi, che deve essere richiesta dallo Stato di esecuzione all'autorità competente del medesimo Stato. Esemplificando, facendo riferimento alla legislazione italiana, l'autorità giudiziaria richiesta potrebbe domandare l'autorizzazione a procedere nei confronti di un Ministro al ramo del Parlamento a cui appartiene[70]. Se l'immunità o il privilegio competono a un altro Stato membro, a un Paese terzo o a un'organizzazione internazionale, l'autorità di emissione può chiedere che vengano revocati all'autorità interessata (art. 5, paragrafo 7, dell'orientamento generale).

Parallelamente alla garanzia preventiva per i dati protetti, viene introdotta dall'orientamento generale una garanzia successiva (art. 12 *bis*, rubricato «limitazione all'uso di dati acquisiti»), il cui procedimento è speculare a quello preventivo. Così, a titolo esemplificativo, nel corso del processo penale italiano dovranno essere dichiarati inutilizzabili e prontamente cancellati dati che si sono rivelati coperti da immunità o privilegi.

La disciplina così tratteggiata, con meccanismi preventivi e successivi, sembra essere un buon connubio tra le diverse esigenze in campo, dal momento che si fornisce un'attenta garanzia agli interessi individuali ma non si frustra del tutto l'interesse statuale alla raccolta delle prove.

Un nuovo art. 7 *bis* normativizza una procedura di notifica allo Stato di esecuzione qualora lo Stato di emissione voglia richiedere la produzione di dati relativi al contenuto di una persona non residente sul proprio territorio nazionale, in quanto i dati relativi al contenuto sono di natura particolarmente sensibile e per loro tramite «le persone possono rivelare i propri pensieri e dettagli sensibili della loro vita privata».

La notifica, trasmessa tanto al prestatore di servizi quanto allo Stato di esecuzione, ha lo scopo di porre in condizione quest'ultimo di comunicare all'autorità di emissione la presenza di immunità, privilegi o lesioni di diritti e interessi fondamentali o violazione delle norme sulla libertà di stampa. Le osservazioni sono volte a consentire allo lo Stato di emissione di tenere in considerazione le citate circostanze come previste dal proprio diritto interno, così da poter adeguare l'ordine alla fattispecie concreta – eventualmente chiedendo all'autorità competente la revoca dell'immunità o del privilegio – ovvero disporre la revoca dello stesso.

È espressamente previsto che, al fine di non ritardare l'esecuzione, la notifica allo Stato non abbia effetto sospensivo (art. 7 *bis*, paragrafo 4, dell'orientamento generale). È necessario sin da subito evidenziare che, come verrà sottolineato *infra* e analogamente a quanto già tratteggiato in tema di manifesta violazione dei diritti

[70] Artt. 5 e 9 l. cost. 16 gennaio 1989, n. 1.

fondamentali, sarebbe più opportuno prevedere una notifica con effetto parzialmente non sospensivo – che obblighi cioè il SP a conservare il dato ma non a produrlo, in attesa della decisione dell'autorità – allo Stato in cui risiede il soggetto nei cui confronti vengono richiesti i dati, che non necessariamente coincide con lo Stato di esecuzione.

Vi è da precisare, inoltre, che la riscrittura dell'art. 8, paragrafo 2, affianca alla modalità di trasmissione dei certificati in forma scritta la necessità che gli stessi siano trasmessi con «modalità sicure e affidabili». È certamente apprezzabile tale ultimo riferimento, dal momento che ogni modificazione, anche minima, dei dati richiesti e trasmessi potrebbe condurre all'inutilizzabilità dei risultati raccolti. Sul punto, si è argomentato in dottrina che la nuova formulazione dell'art. 8, paragrafo 2, potrebbe essere alla base della trasmissione di dati per mezzo di una piattaforma analoga a quella che è in via di sviluppo nei rapporti giurisdizionali tra le autorità giudiziarie dei singoli Stati membri[71]. Un'idea che non pare peregrina e che, soprattutto, nel caso in cui il software fosse sviluppato con le massime garanzie di affidabilità e sicurezza, potrebbe essere un porto sicuro per evitare tutti i problemi che possono essere legati alla posta elettronica, tanto certificata quanto ordinaria (si pensi, a titolo esemplificativo, che le autorità giudiziarie di alcuni Stati non hanno un dominio riferito al ministero della giustizia). In ogni caso, sarebbe stato opportuno uniformare le normative nazionali al rispetto di rigorosi standard tecnici valevoli in tutto il territorio dell'Unione e non limitarsi ad utilizzare formule aperte la cui definizione è rimessa agli interpreti[72].

L'esecuzione dell'EPOC è modificata introducendo un'espressa previsione per mezzo della quale i dati devono essere trasmessi all'autorità di emissione «secondo modalità sicure e affidabili che consentano di stabilire l'autenticità e l'integrità» degli stessi (art. 9, paragrafo 1, dell'orientamento generale)[73]. Una modifica necessaria in considerazione delle disposizioni della Convenzione di Budapest del 2001 sulla criminalità informatica che impone una garanzia di affidabilità e inalterabilità dei dati acquisiti, che se non rispettata conduce all'inutilizzabilità dei dati raccolti[74].

Sul punto vi è da segnalare che la Commissione ha formulato una specifica

---

[71] S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., p. 174.

[72] In tal senso anche L. Gomez Amigo, *Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima*, in *Revista Española de Derecho Europeo*, 2019, 71, p. 31: «*por lo demás, las pruebas electrónicas pueden ser más fáciles de manipular por lo que necesitan garantías adicionales y específicas que permitan mantener la cadena de custodia, asegurando su autenticidad e integridad durante todo el proceso de recogida, conservación, transmisión y entrega de las mismas. Tratándose de un sistema europeo de obtención transfronteriza de pruebas electrónicas sería deseable que la Unión Europea estableciese unas normas mínimas comunes al respecto (que no se contienen en la normativa propuesta por la Comisión), y que garantizarían la admisibilidad de las pruebas electrónicas en el Estado que las solicitó*».

[73] V. Considerando 40 Orientamento generale, cit.

[74] V. artt. 16 e 19 Convenzione di Budapest sul *Cybercrime*.

proposta di regolamento, denominata e-CODEX[75], in virtù della quale nell'ambito dei procedimenti civili o penali possono essere scambiati – per il tramite appunto del sistema e-CODEX (la cui gestione dovrebbe essere affidata all'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA)) – messaggi, dati, documenti e informazioni in modo rapido, sicuro e che permetta di garantire l'identità digitale del mittente e l'avvenuta ricezione di quanto inviato. Se la proposta e-CODEX dovesse essere approvata, potrebbe essere la base anche per lo scambio degli ordini e dei dati tra Stato di emissione e *provider*.

L'orientamento generale codifica anche il principio di specialità, previsto tradizionalmente negli strumenti di mutua assistenza e nel MAE, ma inspiegabilmente assente nell'OEI e nella proposta della Commissione. L'art. 12 *ter* dell'orientamento generale sancisce un divieto di utilizzabilità dei dati ottenuti in procedimenti diversi da quelli per i quali si procede e sono stati ottenuti, ad eccezione di due sole ipotesi. La prima richiama i reati di cui all'art. 5, paragrafi 3 e 4, dell'orientamento generale, analoghi a quelli della proposta della Commissione [76]. La seconda facoltizza l'utilizzabilità dei dati raccolti «al fine di evitare una minaccia grave e immediata per la pubblica sicurezza dello Stato di emissione o i suoi interessi fondamentali» (art. 12 *ter*, paragrafo 1, lett. b))[77].

Il principio di specialità ha il pregio di garantire che i dati richiesti e ottenuti nell'ambito di un procedimento penale siano utilizzabili esclusivamente nell'ambito dello stesso, evitando così che vi possano essere strumentalizzazioni dei nuovi ordini o surrettizie utilizzazioni dei dati raccolti. Le deroghe al principio di specialità, poi,

---

[75] Proposta della Commissione europea di *regolamento del Parlamento Europeo e del Consiglio relativo a un sistema informatizzato di comunicazione per i procedimenti civili e penali transfrontalieri (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726*, del 02 dicembre 2020, COM(2020)712.

[76] Per esigenze di semplicità espositiva si riporta il testo dell'art. 5, paragrafi 3 e 4, Orientamento generale, cit.: «3. L'ordine europeo di produzione per la produzione di dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato e per l'esecuzione di una pena detentiva o di una misura di sicurezza privativa della libertà di almeno 4 mesi.

4. L'ordine europeo di produzione per la produzione di dati relativi alle operazioni o dati relativi al contenuto può essere emesso solo

(a) per i reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni, oppure

(b) per i seguenti reati, se commessi in tutto o in parte a mezzo di un sistema di informazione:

– i reati di cui agli articoli 3, 4 e 5 della decisione quadro 2001/413/GAI del Consiglio;

– i reati di cui agli articoli da 3 a 7 della direttiva 2011/92/UE del Parlamento europeo e del Consiglio;

– i reati di cui agli articoli da 3 a 8 della direttiva 2013/40/UE del Parlamento europeo e del Consiglio;

(c) per i reati di cui agli articoli da 3 a 12 e all'articolo 14 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio;

d) per l'esecuzione di una pena detentiva o di una misura di sicurezza privativa della libertà di almeno 4 mesi disposta per i reati di cui alle lettere a), b) e c) del presente paragrafo».

[77] V. Considerando 56 *bis* Orientamento generale, cit.

possono considerarsi proporzionate poiché insistono su categorie di reati di tendenziale elevata gravità.

L'art. 17 dell'orientamento generale si fa carico del problema dei rimedi che, nella proposta originaria, erano riservati nei confronti dei soli ordini di produzione e rischiava di creare evidenti disparità di trattamento con conseguente lesione del diritto sancito dall'art. 47 della Carta di Nizza. La nuova formulazione dell'art. 17 prevede, al contrario, che siano reclamabili dai soggetti interessati sia gli OCE sia gli OPE, dal momento che il ricorso giurisdizionale, ai sensi del diritto interno, è reso disponibile a «qualsiasi persona i cui dati sono stati ricercati»[78]. Nel nuovo testo, dunque, il rimedio successivo è stato esteso a tutte le posizioni soggettive veicolate per mezzo del regolamento.

Merita, infine, un accenno il sistema delle sanzioni. L'art. 13, paragrafo 3, dell'orientamento generale garantisce che la sanzione pecuniaria irrogabile dagli Stati membri nei confronti dei *provider* inadempienti possa consistere in una somma pari fino al 2% del fatturato mondiale annuo del prestatore di servizi, tenendo conto «di tutte le circostanze pertinenti, quali la natura, la gravità e la durata della violazione, se è stata commessa intenzionalmente o per negligenza, se il fornitore del servizio è stato ritenuto responsabile per analoghe violazioni precedenti e la solidità finanziaria del prestatore di servizi ritenuto responsabile»[79].

L'indicazione di una somma massima della sanzione parametrata al fatturato mondiale non elimina i potenziali rischi di *forum shopping* evidenziati in precedenza, in quanto le legislazioni nazionali rimangono libere di imporre sanzioni proprie nel limite del citato 2%. A ciò si aggiunga che non è dato comprendere sulla base di quali criteri quantificare il fatturato "mondiale" del *provider*, anche in considerazione delle complesse strutture societarie in cui i *provider* sono inserite. Per esemplificare, se la società Alfa ha la sede legale della capogruppo in Germania, sedi nazionali delle controllate in ogni Stato membro dell'UE e detiene i server in Olanda, il fatturato mondiale della capogruppo verrà calcolato sulla base del bilancio della *holding*, delle società statali "figlie" o di quella a cui materialmente sono riferiti i server?

Una domanda a cui non è certo semplice fornire una risposta univoca e che potrebbe essere oggetto di attenta discussione nel tavolo trilaterale Commissione-Consiglio-Parlamento.

5. Il Parlamento Europeo ha assegnato la discussione della proposta della Commissione alla commissione LIBE (*"Committee on civil liberties, justice and home*

[78] V. anche Considerando 54 Orientamento generale, cit.

[79] Considerando 45 *bis* Orientamento generale, cit.

affairs")[80] e alla deputata Birgit Sippel è stato affidato il compito di relatrice. Il 24 ottobre 2019 è così stato presentato un progetto di relazione contenente numerosi emendamenti che insistono su una più ampia tutela dei diritti fondamentali (progetto Sippel)[81]. Il progetto Sippel[82] sembra abbandonare l'ottica del mutuo riconoscimento tra Stati[83], voluta fortemente dalla Commissione e ripresa – ma in qualche modo temperata – dal Consiglio, a favore di una maggiore garanzia dei diritti del singolo[84].

Nelle motivazioni del progetto Sippel si legge che si è di fronte a «un'interpretazione atipica del concetto di riconoscimento reciproco, che consente all'autorità di emissione di rivolgersi ai prestatori di servizi in un'altra giurisdizione senza coinvolgere automaticamente le autorità dell'altro e degli Stati interessati» e che vi è l'«introduzione dell'extraterritorialità o elusione di prerogative fondamentali dello Stato»[85]. Per quanto possa sembrare atipico ed eccentrico per la cooperazione internazionale comunicare direttamente con un soggetto privato, in realtà la proposta della Commissione non fa altro che potenziare la strada del mutuo riconoscimento intrapresa oltre 20 anni orsono ed esaltare quella fiducia reciproca tra gli Stati membri che dovrebbe caratterizzare i rapporti infra-europei. Invero, come visto in precedenza, è possibile sostenere che il mutuo riconoscimento non avvenga tramite autorità giudiziarie, bensì sia il frutto di una disposizione legislativa specifica, ossia il regolamento.

Si è successivamente addivenuti alla relazione legislativa, adottata in data 11

---

[80] La Commissione LIBE, a sua volta, ha commissionato uno studio dedicato al tema: M. Böse, *An assessment of the Commission's proposals on electronic evidence*, Bruxelles, 2018.

[81] Progetto di Relazione Sippel sulla proposta di *regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* del 24 ottobre 2019, COM(2018)0225 – C8-0155/2018 – 2018/0108(COD).

[82] Saluta con favore il Progetto Sippel T. Christakis, *E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report*, in *www.europeanlawblog.eu*, 21 gennaio 2020; T. Christakis, *Lost in notification? Protective logic as compared to efficiency in the European parliament's e-evidence draft report*, in *www.crossborderdataforum.org*, 07 gennaio 2020; T. Christakis, *E-evidence: the way forward (Summary of the Workshop held in Brussels on 25 Septembre 2019)*, in *www.europeanlawblog.eu*, 06 novembre 2019.

[83] È stato evidenziato come "*The Report is not founded in 'absolute' mutual trust (as the Commission's version) but on the idea that efficiency arguments should not override the need to protect fundamental rights*" (T. Christakis, *E-Evidence in the EU Parliament*, cit.).

[84] Lo stravolgimento dell'impianto originario ha provocato una forte reazione della Commissione che ha portato a un confronto istituzionale inedito all'interno dell'Unione. Più precisamente, pare che la Commissione abbia trasmesso ad alcuni portatori di interessi selezionati un report altamente critico del Progetto Sippel per dimostrare che quest'ultimo avrebbe un enorme impatto negativo sull'efficienza della raccolta delle *e-evidence*. In dottrina v. T. Christakis, *Lost in notification?*, cit. L'impianto del Parlamento europeo è apprezzato da taluni *stakeholders* nel *Joint Statement encouraging EU legislators to fight for fundamental righs protections in e-Evidence legislation*, pubblicato a Bruxelles il 6 gennaio 2020, reperibile al seguente link: Joint Statement Encouraging EU Legislators to Fight for Fundamental Rights Protections in e-Evidence Legislation | BSA | The Software Alliance.

[85] Progetto di Relazione Sippel, cit., p. 150.

dicembre 2020, in cui è stata recepita la maggior parte degli emendamenti presentati (relazione della Commissione LIBE)[86]. Pochi giorni dopo l'approvazione della predetta relazione, il 14 dicembre 2020, la Commissione LIBE ha annunciato nella seduta plenaria del Parlamento Europeo, ai sensi dell'art. 71 del regolamento dello stesso, la decisione di intraprendere negoziati interistituzionali al fine di addivenire a un testo consolidato del nuovo regolamento; decisione confermata dalla seduta plenaria del 16 dicembre 2020.

La relazione della Commissione LIBE si sviluppa sulla massima partecipazione dello Stato di esecuzione agli ordini, al fine di consentire a quest'ultimo di «poter rifiutare il riconoscimento o l'esecuzione di un ordine, qualora tale rifiuto sia basato sui motivi specifici elencati in un nuovo articolo del progetto di relazione, in linea con i motivi adottati nella direttiva 2014/41/UE» [87]. Per tale motivo è prevista la contemporanea notifica dell'EPOC e dell'EPOC-PR tanto al *provider* quanto allo Stato di esecuzione [88], sebbene sia previsto che l'autorità di esecuzione possa rifiutare esclusivamente un EPOC ma non anche un EPOC-PR (artt. 8, 9 e 19 relazione della Commissione LIBE). Più nello specifico, lo stato di esecuzione conferma l'ordine o lo respinge sulla base di motivi tassativi indicati dal regolamento al nuovo art. 10 *bis*[89]; all'inadempienza la relazione della Commissione LIBE fornisce il valore di silenzio-assenso e il *provider*, che nel frattempo deve conservare i dati richiesti ma senza produrli, dovrà eseguire l'ordine (artt. 8 *bis* e 9 della relazione della Commissione LIBE)[90].

Una novità assoluta contenuta nel progetto Sippel riguardava la notifica dell'ordine di produzione anche allo Stato in cui è residente il soggetto nei confronti del quale si ricercano i dati (art. 7, paragrafo 1 *quater*, del progetto Sippel) [91]. Esemplificando, se l'autorità italiana richiede a un *provider* stabilito in Irlanda i dati di un soggetto residente in Francia, l'Italia dovrà notificare l'ordine al *provider*, all'Irlanda e alla Francia. E ciò al fine di consentire all'autorità giudiziaria dello Stato di residenza dell'interessato di comunicare allo Stato di esecuzione i propri dubbi sulla legittimità dell'ordine ai sensi del nuovo art. 10 *bis* del progetto Sippel, il quale a sua volta deve comunicarli allo Stato di emissione (art. 9, paragrafo 2 *ter*, del progetto Sippel)[92]. E il

[86] Trattasi del progetto A9-0256/2020 «****I Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)0225 – C8-0155/2015 – 2018/0108(COD))*»

[87] Progetto di Relazione Sippel, cit., p. 151.

[88] Considerando 37 relazione della Commissione LIBE, cit.

[89] Considerando 42 *ter* relazione della Commissione LIBE, cit.

[90] Considerando 40 e 40 *bis* relazione della Commissione LIBE, cit.

[91] Considerando 37 *bis* Progetto di Relazione Sippel, cit.

[92] Considerando 40 *ter* Progetto di Relazione Sippel, cit.

tutto entro 10 giorni[93].

Fortunatamente questo farraginoso meccanismo non è stato recepito nella relazione della Commissione LIBE. Tuttavia, in relazione alla necessità della notificazione e al soggetto destinatario si impongono alcune riflessioni, dal momento che le proposte della Commissione, del Consiglio e del Parlamento, per le ragioni che si sono viste, non sembrano del tutto condivisibili.

Così come argomentato in dottrina[94], è innanzitutto necessario considerare che, nella maggior parte dei casi, probabilmente l'autorità procedente emetterà un ordine in relazione a un soggetto residente sul suo territorio. In tal caso, la tutela dei diritti fondamentali della persona nei confronti della quale si stanno svolgendo le indagini (o di altro soggetto) è rimessa all'autorità che ha messo l'ordine, che è allo stesso tempo autorità richiedente e procedente, con la conseguenza che una notifica allo Stato di esecuzione si rivelerebbe meramente superflua e dilatoria (anche in considerazione del fatto che la tutela della riservatezza è uniformata in tutta Europa dal regolamento 2016/679/UE – c.d. GDPR). Invero, da un lato, il SP sarebbe sottoposto al GDPR e al nuovo regolamento sulle *e-evidence* e non vedrebbe lese le proprie prerogative; dall'altro, tutti i diritti dell'indagato sarebbero tutelati per mezzo dei rimedi processuali presenti nello stato di emissione.

Al contrario, vi è la possibilità – minore ma non certo inesistente – che l'indagato risieda in uno Stato diverso da quello di emissione, sia esso lo Stato di esecuzione o altro Stato dell'Unione. In tal caso, al fine di garantire i diritti dell'indagato, sarebbe opportuno prevedere la notifica allo Stato di residenza, concedendo a questo un termine (breve) per opporsi all'ordine emesso. Nelle more di un'eventuale decisione di dissenso o silenzio-assenso, il *provider* dovrebbe conservare i dati richiesti, al fine di trasmetterli all'autorità richiedente in caso di mancata opposizione dello Stato notificato.

Ragionando nei termini sopra indicati, si può ritenere che vi sia un bilanciamento tra la fondamentale esigenza di tutela dei diritti fondamentali e le ragioni di celerità sottese al nuovo strumento. La persona nei confronti della quale vengono richiesti i dati avrà la massima garanzia dello Stato in cui risiede, che può o meno coincidere con quello di emissione; al contrario, infatti, è più difficile comprende quale possa essere l'interesse dello Stato di esecuzione qualora la persona nei cui confronti si richiedono i dati non sia presente sul suo territorio.

I motivi di non riconoscimento di un EPOC previsti dal summenzionato art. 10

[93] Avalla una simile (e opinabile) scelta T. Christakis, *E-Evidence in the EU Parliament*, cit., secondo il quale «*the introduction in the E-Evidence package of the concept of the "affected State", as Sippel suggests, will permit to "adapt" in an appropriate way in the digital world protections that already existed traditionally "in the physical world" under MLA systems*».

[94] T. Christakis, *"Big Divergence of Opinions on e-Evidence in the EU Council*, op. cit.

bis della relazione della Commissione LIBE sono simili a quelli annoverati nell'art. 11 della direttiva OEI e concernono soli motivi di legittimità, mentre quelli di merito – inerenti cioè la necessità e la proporzionalità dell'ordine – potranno essere reclamati solo nello Stato di emissione[95-96].

La reclamabilità nello Stato di emissione dei motivi di merito degli ordini si pone in linea con gli strumenti di cooperazione giudiziaria a livello europeo già presenti, in quanto l'autorità procedente ha a disposizione tutti gli elementi giuridici e fattuali per valutare la necessità e la proporzionalità dello strumento.

Apprezzabile è la proposta di prevedere un compendio probatorio minimo (criterio della c.d. *high probability*[97]) ai fini dell'emissione dell'ordine, con lo scopo di scongiurare il rischio di indagini preventive e meramente conoscitive, sprovviste di un «certo livello di sospetto che il reato sia stato commesso» (artt. 5, paragrafo 2, e 6, paragrafo 2, della relazione della Commissione LIBE)[98].

Il criterio della *high probability* – equivalente indicativamente ai nostri gravi indizi di colpevolezza delle misure cautelari o ai gravi indizi di reato delle intercettazioni – sembra voler assicurare i principi di proporzionalità e necessità, codificando espressamente una presunzione assoluta di mancanza degli stessi in assenza di sufficienti motivi per ritenere che sia stato commesso un reato, pur se un procedimento penale è già stato avviato.

Meritevole di attenzione è anche la sensibilità che la relazione della

[95] Art. 17, paragrafo 3 *bis*, relazione della Commissione LIBE.

[96] Più nel dettaglio, i motivi di legittimità riguardano: le violazioni del *ne bis in idem*; l'incompatibilità con gli obblighi di cui all'art. 6 TUE; la presenza di immunità o privilegi; la violazione dell'art. 5 del regolamento relativi alle condizioni di emissione dell'OPE; la lesione di interessi essenziali per la sicurezza nazionale, la messa in pericolo della fonte delle informazioni o l'uso di informazioni riguardanti attività di *intelligence* specifica; la commissione di reati al di fuori del territorio dello Stato di emissione e lo Stato di esecuzione non consente l'azione penale per gli stessi reati; la violazione del principio di doppia incriminazione, ad eccezione della lista dei 32 reati già prevista per MAE e OEI; la limitazione a una categoria di reati punibili entro una soglia di pena detentiva massima di tre anni; il contrasto con il diritto applicabile di un Paese terzo. Viene anche richiamata la clausola in tema di reati tributari che impedisce di non riconoscere l'ordine se una tassa o un'imposta non sono previste dallo Stato di esecuzione.

[97] J.H. Jeppesen-G. Nojeim, *Assessing the European Commission's E-Evidence Proposals*, op. cit.

[98] V. Considerando 29 relazione della Commissione LIBE, cit.: «L'ordine europeo di produzione dovrebbe essere emesso solo se è necessario e proporzionato, tenendo conto dei diritti della persona indagata o imputata e della gravità del reato. La valutazione dovrebbe considerare se ***l'ordine avrebbe potuto*** essere disposto alle stesse condizioni in un caso interno analogo, se sussistono motivi sufficienti per ritenere che sia stato commesso un reato, se quest'ultimo è sufficientemente grave da giustificare la produzione transfrontaliera di dati e se le informazioni richieste sono pertinenti ai fini dell'indagine. L'ordine dovrebbe essere limitato a quanto strettamente necessario per raggiungere il legittimo obiettivo di ottenere i dati pertinenti e necessari che dovranno servire da prova solo nella singola fattispecie e dovrebbe essere limitato ai dati relativi a determinate persone aventi un legame diretto con il procedimento in questione. L'esistenza di un legame diretto tra la persona i cui dati sono ricercati e lo scopo del procedimento deve poter essere dimostrata in qualsiasi momento». V. anche Considerando 36 relazione della Commissione LIBE, cit.

Commissione LIBE ha nei confronti dell'indagato e dell'imputato, dal momento che facoltizza questi ultimi, anche per mezzo del proprio difensore, a richiedere l'emissione di un OPE o di un OCE conformemente alla procedura nazionale (art. 1, paragrafo 1 *bis*, della relazione della Commissione LIBE). Così come in tema di OEI, dunque, viene dato spazio alle indagini difensive, le quali tuttavia pare non possano essere effettuate dal difensore autonomamente in assenza dell'intervento dell'autorità pubblica: quest'ultima, invero, sembra l'unica ad avere un simile potere, che al più può essere sollecitato dal difensore dell'imputato[99].

Ci si può domandare, tuttavia, se non sia opportuno che il difensore possa azionare direttamente lo strumento per il tramite delle indagini difensive previste dalle legislazioni di alcuni Paesi membri dell'UE.

La risposta, almeno al momento, può non essere né negativa né positiva a seconda della scelta circa il ruolo che il pubblico ministero ha nell'emissione degli ordini.

Può essere negativa qualora si decida di autorizzare il pubblico ministero a richiedere OCE e OPE senza intervento di un giudice. Il pubblico ministero, infatti, è il "naturale antagonista" dell'indagato e, così statuendo, si potrebbe sostenere che si violino il diritto di difesa e il principio di parità delle armi previsti dall'art. 6 CEDU[100].

Se, al contrario, si opta per una scelta volta ad affidare al solo giudice l'emissione degli ordini, rimettendo al pubblico ministero un mero ruolo di impulso (salvo eventualmente casi di urgenza debitamente documentabili), allora in questo caso la scelta di rimettere un mero potere di istanza al difensore può essere valutato positivamente.

Si segnala, in ogni caso, che la persona offesa non è stata inserita nel novero dei soggetti che possono richiedere l'emissione dell'ordine: esclusione che – sebbene in linea con quanto previsto dall'art. 1, paragrafo 3, direttiva 2014/41 UE[101] – sembra francamente irragionevole, anche alla luce del peso nel processo che la persona offesa ha acquistato negli ultimi anni a livello unionale[102].

---

[99] Per un approfondimento sulle indagini difensive transnazionali, ma in tema di OEI, v. M. Caianiello, *L'OEI dalla direttiva al Decreto n. 108 del 2017*, in M. Daniele-R.E. Kostoris (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transazionale delle prove nel d.lgs. n. 108 del 2017*, Torino, 2018, pp. 33-37; P. Spagnolo, *Il procedimento di emissione dell'OEI*, in M. Daniele-R.E. Kostoris (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transazionale delle prove nel d.lgs. n. 108 del 2017*, Torino, 2018, pp. 93-96.

[100] V., *ex multis*, Corte europea dei diritti dell'uomo, Granze Camera, sentenza del 19 settembre 2017, ricorso n. 35289/11, *Regner c. Repubblica Ceca*, par. 146 ss.

[101] La direttiva OEI prevede la possibilità per il solo indagato o imputato, e il relativo difensore, di richiedere all'autorità giudiziaria indagini difensive. L'assenza della vittima di reato nella direttiva 2014/41/UE cit. è evidenziata da M. Cagossi, *Un illustre assente: la vittima del reato nell'ordine europeo di indagine penale*, Torino, 2016, pp. 119-125.

[102] V., in tema di vittime di reato, la direttiva 2012/29/Ue del Parlamento Europeo e del Consiglio, *che istituisce*

Di pregevole interesse torna ad essere l'espressa previsione di «inammissibilità» dei dati acquisiti in violazione del regolamento e della immediata cancellazione degli stessi, anche qualora non siano più necessari ai fini del procedimento (art. 11 *quater* relazione della Commissione LIBE)[103].

Si può notare, alla luce della presente analisi, come la relazione della Commissione LIBE abbia voluto evitare il «trasferimento delle valutazioni dei diritti fondamentali a società private», al fine di evitare «il rischio di privatizzare la cooperazione dell'Unione in materia di diritto penale», così sovvertendo il proposito originario che era alla base della proposta della Commissione e seguito, pur con modificazioni, da parte del Consiglio.

6. Al momento non vi è unitarietà di vedute circa l'opportunità di una cooperazione diretta pubblico-privato[104].

In ogni caso, la proposta di regolamento della Commissione, così come modificata dal Consiglio, pur perfettibile in taluni punti, pare fornire il giusto punto di equilibrio tra le istanze securitarie della Commissione e quelle garantiste del

norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI, del 25 ottobre 2012, in GUUE L. 315 del 14 novembre 2012, pp. 57 ss., la quale purtroppo non prevede alcuna disposizione in tema di indagini difensive della persona offesa.

[103] Considerando 43 *quater* e 43 *quinquies* relazione della Commissione LIBE, cit. Vi è da segnalare, tuttavia, che parte della dottrina – pur evidenziando come la proposta della Commissione non si faccia carico della questione delle prove acquisite illegalmente – ritiene che «l'ammissibilità reciproca delle prove tra gli Stati membri rientra tra le materie elencate all'articolo 82, paragrafo 2, con riferimento alle quali, come si diceva, è previsto un intervento normativo da parte dell'Unione solo attraverso le direttive» (A. Rosanò, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea*, op. cit., p. 17).

[104] Questa differenza di vedute, secondo parte della dottrina, è dovuta a due fattori: «*first, the differences among member states' regulation of domestic and foreign service providers. Second, due to the absence of rules on whether requests issued directly to a service provider in another country are voluntary or mandatory for the service provider being addressed*» (S. Vazquez Maymir, *Anchoring the Need to Revise*, op. cit., p. 5).

Vi è, peraltro, chi teorizza un approccio federale, con la rimessione a un organo giurisdizionale europeo unico della tematica della *e-evidence*: «nello scenario "liquido" delle indagini informatiche, l'approccio meno problematico passa attraverso la creazione, in una logica federale, di un unico organo giurisdizionale europeo deputato a svolgere i controlli che la proposta vorrebbe affidare ai *provider*. Un organo a cui le autorità giudiziarie nazionali dovrebbero rivolgere gli ordini di conservazione e di produzione, e a cui i *provider* che prestino i loro servizi nell'Unione dovrebbero trasmettere le informazioni rilevanti in loro possesso. [...] Non sarebbe, naturalmente, una soluzione priva di difetti. Dovrebbe essere un organo in grado di operare con la massima efficienza, capace di soddisfare in tempi ragionevolmente rapidi richieste provenienti da ogni parte del globo. A questo fine potrebbe forse essere utile prevedere, nei casi di urgenza, una procedura velocizzata: gli ordini che non apparissero manifestamente arbitrari potrebbero essere immediatamente eseguiti, per poi venire sottoposti ad un più approfondito vaglio successivo all'esecuzione, decretando *ex post* l'inutilizzabilità nello Stato di emissione dei dati raccolti qualora quest'ultimo avesse esito negativo40. In ogni caso, per quanto possa apparire difficile da realizzare, sarebbe una soluzione di gran lunga preferibile alla logica privatistica postulata dalla proposta di regolamento, suscettibile di aprire scenari dalle implicazioni davvero inquietanti per la tutela dei diritti» (M. Daniele, *L'acquisizione delle prove dai* service provider, op. cit., pp. 1292-1293).

Parlamento; essa può dunque divenire un ulteriore tassello nella costruzione di uno spazio europeo di giustizia, libertà e sicurezza comune a tutti gli Stati membri, utile in particolar modo in una società digitalizzata ove lo sviluppo della tecnologia è inarrestabile.

Gli strumenti processuali a disposizione delle autorità giudiziarie, infatti, non possono rimanere ancorati al passato, ma dovrebbero essere aperti alle sfide che le nuove tecnologie apportano in tutti i settori della vita sociale. E tra le sfide insite dell'informatizzazione vi è quella di acquisire dati la cui immaterialità riverbera i propri effetti sulla circolazione degli stessi, che non si arresta ai confini nazionali, ma li varca e si espande potenzialmente a tutto il globo.

Il venir meno della territorialità del dato apre agli interrogativi sulla loro acquisizione transfrontaliera che, quantomeno a livello unionale, possono essere sciolti dalla reciproca fiducia che gli Stati membri hanno consolidato e rafforzato nel corso degli ultimi decenni.

È proprio sulla base di un clima di fiducia che si fonda la proposta della Commissione e che, pertanto, «non può non essere salutata con favore»[105], dal momento che può essere «un rilevante punto di svolta nel processo di adeguamento degli strumenti di formazione e circolazione probatoria in ambito transnazionale alle nuove sfide della società dell'informazione digitale»[106]. Un punto di svolta che, peraltro, avrebbe un vantaggio collaterale consistente nella riduzione del carico giudiziario a livello europeo, anche in considerazione del fatto che la normativa sugli OPE «*is part of a wider trend of transferring enforcement tasks to private actors*»[107]. Sulla base di un "tacito riconoscimento" (*rectius* di un riconoscimento previsto dal regolamento), in altre parole, si potrebbe garantire un maggior rispetto del principio della ragionevole durata del processo (art. 6 CEDU), in considerazione del peso che la prova elettronica acquisirà nei prossimi anni. Inoltre, in dottrina è stato evidenziato come la cooperazione diretta autorità-*provider* comporti una maggiore trasparenza e, conseguentemente, rafforzi la certezza del diritto[108].

---

[105] M. Gialuz-J. Della Torre, *Lotta alla criminalità nel* cyberspazio, cit., p. 291. V. anche O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence, cit., p. 7., secondo cui «nel complesso, la proposta di regolamento e-Evidence merita sicura approvazione e pare indirizzarsi nella giusta direzione».

[106] O. Pollicino-M. Bassini, *La proposta di regolamento* e-Evidence, cit., p. 1. Sul punto è stato anche evidenziato che «*there is little doubt that within a clear legal framework that defines the limits and safeguards governing the modalities under which public authorities may lawfully obtain data the overall judicial system will benefit in terms of efficiency and deliverability. […] The lengthy process to finally receive or access evidence through judicial cooperation was marked as the most common complication by practitioners from law enforcement and judicial authorities*» (L. Buono, *The Genesis of the European Union's New Proposed Legal Instrument(s)*, op. cit., p. 312).

[107] S. Tosza, *All evidence is equal, but electronic evidence is more equal than any other*, op. cit., p. 180.

[108] Per dirla con le parole dell'Autrice, «*furthermore, transparency for individuals on the level of cooperation by service providers with authorities will likewise improve, hence furthering legal certainty*» (N.A. Smuha, *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency*,

Si è certamente di fronte a uno schema del tutto nuovo di collaborazione giudiziaria: si abbandona, nella proposta della Commissione e nell'orientamento generale del Consiglio, la nozione di "decisione giudiziaria" prevista dalla disciplina sul MAE e sull'OEI, il pubblico interagisce con il privato e la poliedricità dello strumento «non postula più indefettibilmente, come nell'impostazione tradizionale, azioni separate ma coordinate di due entità statali diverse, ma contempla nuovi schemi, inediti, ora riconducibili al principio del mutuo riconoscimento delle decisioni giudiziarie, ora esulanti dallo stesso, ora realizzanti una sua particolare declinazione»[109].

Il diverso approccio del Parlamento europeo denota una certa diffidenza nei confronti degli Stati membri e introduce un necessario vaglio preventivo dell'autorità giudiziaria dello Stato di esecuzione, propedeutico a un'eventuale trasmissione dei dati a cura del *service provider* direttamente allo Stato di emissione dell'ordine, atteso che vi potrebbe essere il rischio di svilire i diritti fondamentali dei singoli a favore delle esigenze processuali nell'accertamento dei reati.

Con la relazione della Commissione LIBE si è, dunque, di fronte a un ibridismo che vede, da un lato, la proposta della Commissione con il rapporto diretto pubblico-privato, privo di un filtro preventivo dell'autorità giudiziaria dello Stato di esecuzione; dall'altro la direttiva OEI che postula un rapporto tra le sole autorità dello Stato di emissione e di esecuzione.

Ragionando nei termini della relazione della Commissione LIBE, il regolamento potrebbe sembrare quasi superfluo, dal momento che, riprendendo in larga parte i contenuti della direttiva OEI, perde quelle «caratteristiche di maggiore "appetibilità" in termini di rapidità ed efficienza di acquisizione della prova elettronica»[110] per cui gli ordini erano nati. Per tale motivo la direzione intrapresa dalla Commissione LIBE[111], che affievolisce la celerità del procedimento e la fiducia tra Stati, potrebbe trovare una più opportuna *sedes materiae* all'interno della direttiva OEI.

In realtà, come evidenziato in dottrina, la proposta della Commissione, a differenza delle preoccupazioni veicolate dalla relazione della Commissione LIBE sull'incisione dei diritti fondamentali, ha «il pregio di limitare l'intervento dell'autorità giudiziaria, senza però vanificare né le garanzie proprie del diritto di difesa, né l'efficacia dello strumento di indagine e la salvaguardia del dato digitale [...]. Il testo del regolamento si caratterizza positivamente per il contemperamento tra opposti diritti ed esigenze, e si fa apprezzare laddove distingue tra diverse categorie di dati,

in *European Criminal Law Review*, 2018, p. 19).

[109] R.M. Geraci, *La circolazione transfrontaliera*, cit., p. 1355.

[110] R. Pezzuto, *Accesso transazionale alla prova elettronica nel procedimento penale*, op. cit., p, 69.

[111] In realtà, la discussione all'interno della Commissione LIBE è piuttosto accesa e il progetto Sippel è avversato da una parte consistente dei gruppi parlamentari che la compongono.

modulando l'emissione degli ordini in relazione al diritto oggetto di limitazione»[112].

Come si è visto, tuttavia, anche la proposta della Commissione è perfettibile e, al tavolo di discussione trilaterale Commissione-Consiglio-Parlamento, sarebbe auspicabile che si giungesse a un testo la cui base poggi sulla proposta, modificata da taluni opportuni emendamenti proposti dal Consiglio e dal Parlamento. Tra questi si possono annoverare: 1) la previsione del principio del *ne bis in idem* internazionale in situazioni di contemporanea pendenza di due procedimenti penali per la medesima vicenda; 2) l'utilizzabilità dei dati raccolti per l'individuazione di soggetti latitanti, soggetti a misura cautelare custodiale ovvero condannati a una pena o una misura di sicurezza privative della libertà personale della durata di almeno 4 mesi; 3) la richiesta allo Stato di esecuzione di revoca delle immunità o dei privilegi e la loro inutilizzabilità se l'esistenza degli stessi è scoperta successivamente alla consegna; 4) la trasmissione dei dati allo Stato di emissione secondo modalità sicure e affidabili che consentano di stabilirne l'autenticità e l'integrità; 5) l'introduzione del principio di specialità, grande assente già nell'OEI; 6) la reclamabilità tanto degli OPE quanto degli OCE; 7) la necessità di un compendio probatorio minimo ai fini dell'emissione dell'ordine; 8) la previsione dell'inutilizzabilità dei dati acquisiti in violazione del regolamento e la loro immediata cancellazione qualora non siano più necessari ai fini del procedimento; 9) la previsione di un diritto della difesa dell'indagato e della persona offesa di richiedere l'emissione di un ordine.

In conclusione, dunque, si auspica che venga mantenuto l'impianto originario proposto dalla Commissione, migliorato con alcuni non secondari interventi suggeriti da Consiglio e Parlamento.

[112] E. Colombo, *Ordini europei di produzione e di conservazione*, cit., p. 2729.